MINISTERO DELLA CULTURA

DIGITAL LIBRARY
Istituto centrale per la digitalizzazione del patrimonio culturale

IPaC
Infrastruttura e servizi digitali per il Patrimonio Culturale

IAM - Onboarding Applicativi e modalità di autenticazione

agosto 2024

Tabella 1 - Tabella delle versioni

VERSIONI			
DATA	**VERSIONE**	**DESCRIZIONE**	**CAP/SEZ. MODIFICATI**
27/08/2024	1.0		

INDICE

Introduzione

Il presente documento descrive le specifiche per l'on-boarding 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.

Acronimi e Glossario

DEFINIZIONE/ACRONIMO	DESCRIZIONE
IAM	Identity and Access Managment
SP	Service Provider
IdP	Identity Provider
OIDC	OpenID Connect
JWT	JSON Web Token

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 seguente excel ed inviarlo a:

MicroservicesIntegration@almaviva.it;
M.Savoia@almaviva.it;
F.Farroni@almaviva.it;
C.Zotti@almaviva.it;
a.digiovanni@almaviva.it;
c.cuomo@almaviva.it

non compilare - campi in risposta

Nome Application SP	Modalità di Autenticazione			
	OIDC/OAUTH2 - CLIENT CREDENTIAL (M2M)	OIDC/OAUTH2 - CODE (M2W)	User (o LDAP MiC o Email) / Psw	SPID/CIE
stringa breve indicativa dell'applicazione	SI | NO	SI | NO	SI | NO	SI | NO
stringa breve indicativa dell'applicazione	SI | NO	SI | NO	SI | NO	SI | NO
stringa breve indicativa dell'applicazione	SI | NO	SI | NO	SI | NO	SI | NO

Nome Tenant COLLAUDO	AMBIENTE COLLAUDO					
	Callback URL diversa da regexp=(.*)	URL Logout	Necessità gestione utenti UserStore Primario	Utenza		Client_id / Client_secret
				USR	PSW	
coll.ispc.it | coll.icar.it | coll.cloud.sbn.it	1 o n callback URL	*opzionale*	SI | NO			
coll.ispc.it | coll.icar.it | coll.cloud.sbn.it	1 o n callback URL	*opzionale*	SI | NO			
coll.ispc.it | coll.icar.it | coll.cloud.sbn.it	1 o n callback URL	*opzionale*	SI | NO			

Nome Tenant PRODUZIONE	AMBIENTE PRODUZIONE					
	Callback URL diversa da regexp=(.*)	URL Logout	Necessità gestione utenti UserStore Primario	Utenza		Client_id / Client_secret
				USR	PSW	
ispc.it | icar.it | iccu.it	1 o n callback URL	*opzionale*	SI | NO			
ispc.it | icar.it | iccu.it	1 o n callback URL	*opzionale*	SI | NO			
ispc.it | icar.it | iccu.it	1 o n callback URL	*opzionale*	SI | NO			

IAM-ECOMiC-Onboarding Applicativi_v2.0.x

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:

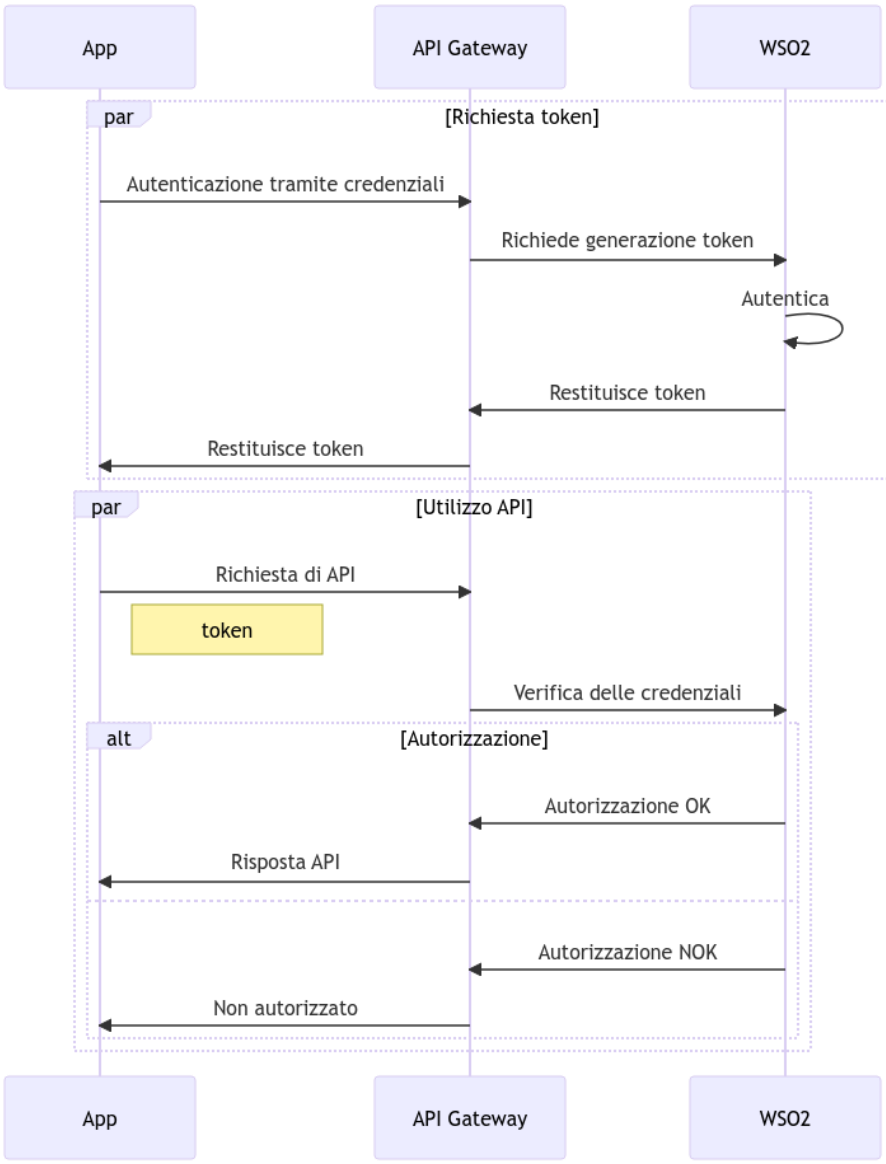
Campo JWT	Descrizione
Sub	Soggetto della utenza in SPID e CIE il codice fiscale
given_name	Nome
family_name	Cognome
fiscalNumber	Codice Fiscale
email	Email del utente (n.b. CIEID non ha email)

Sono attualmente disponibili le seguenti modalità di autenticazione

- M2M
- M2W
- Utenze personali
    - Username/password (lo username può essere anche una e-mail)
    - SPID
    - CIE
    - eIDAS (in fase di sviluppo)

Autenticazione M2M

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



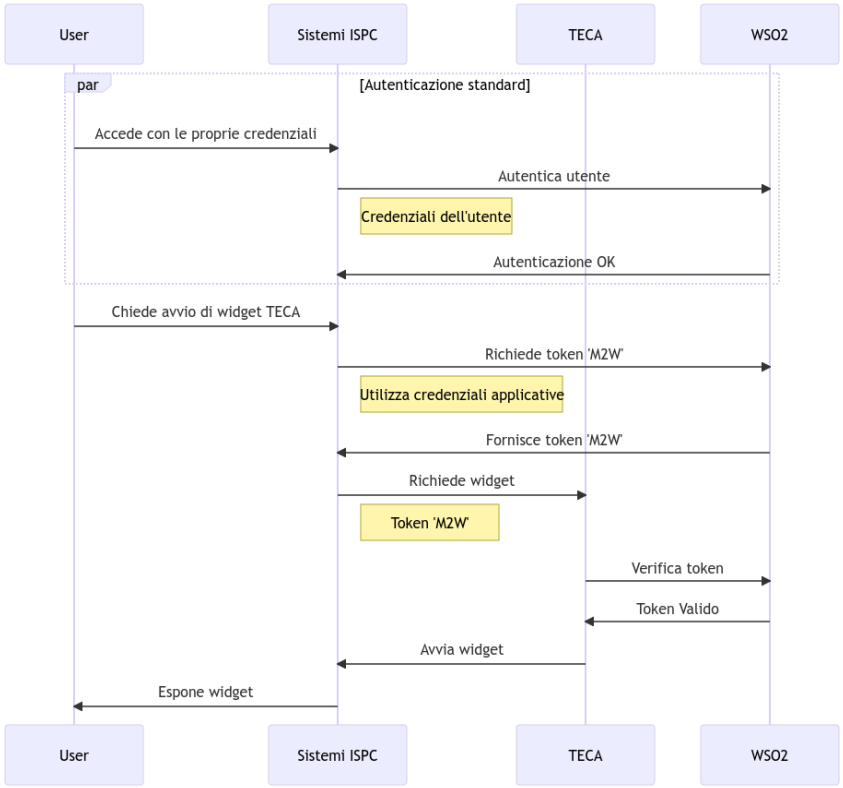
Autenticazione M2W

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:

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 Machine to Widget 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.



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

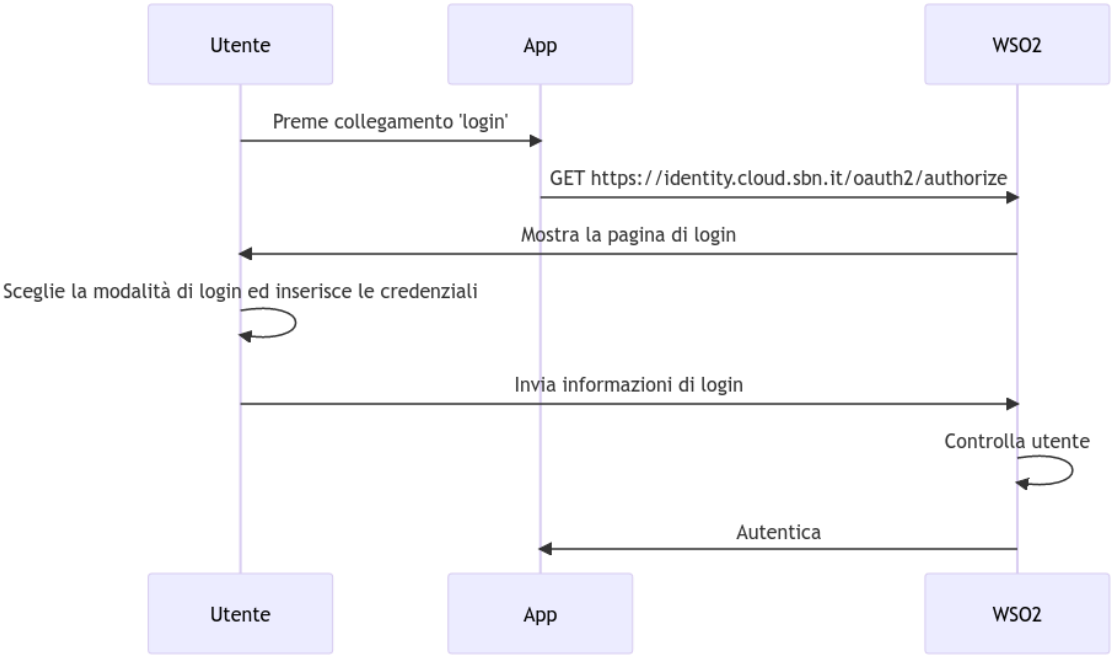
Tale richiesta deve essere corredata dalle seguenti informazioni:

- **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:

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')

Di seguito il generico sequence diagram della fase di autenticazione:

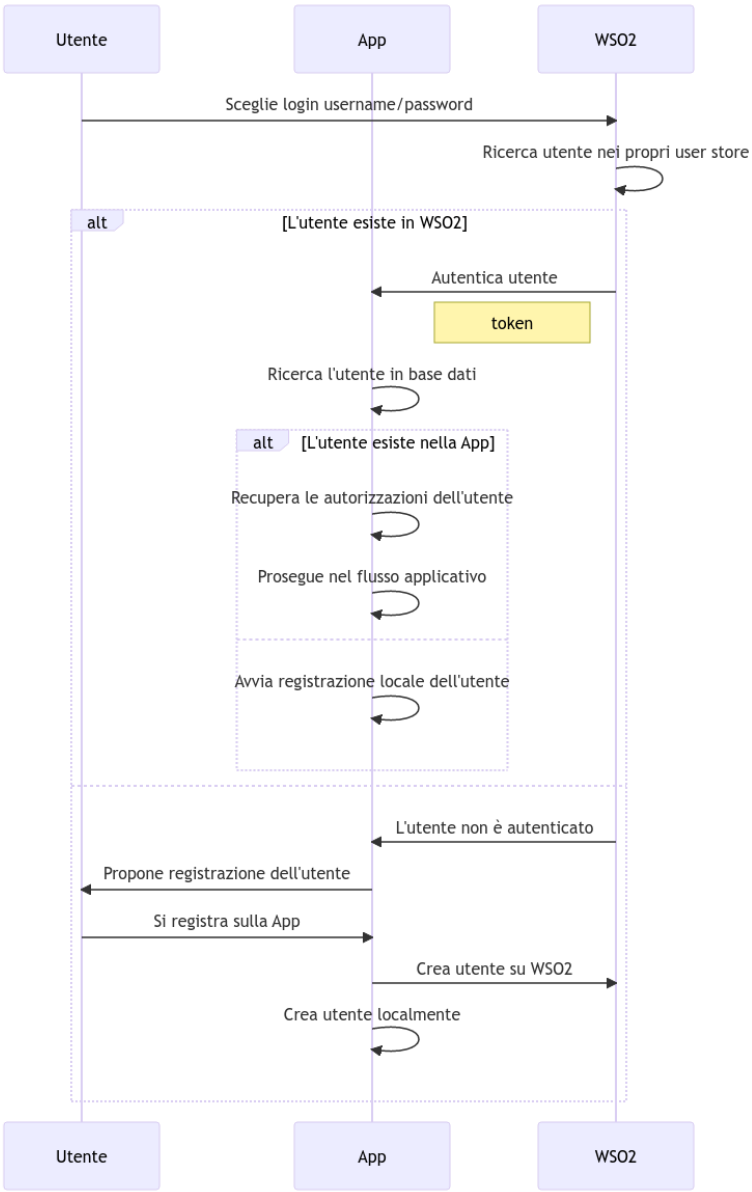


L'utente può autenticarsi tramite le seguenti modalità:

- username/password (ministeriali e non)
- SPID
- CIE
- eIDAS (al momento non disponibile -in fase di sviluppo)

Autenticazione tramite username e password

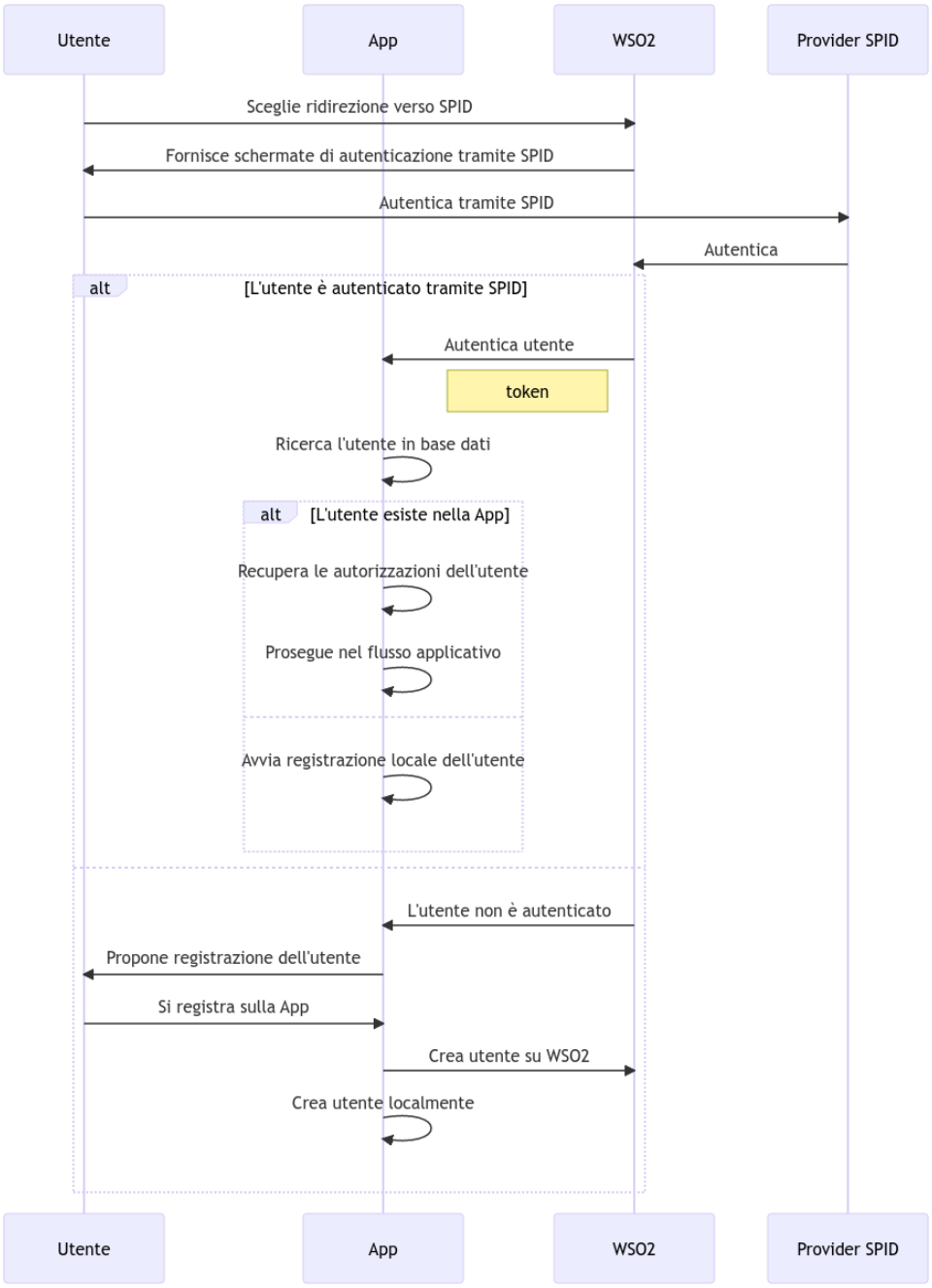
Di seguito il sequence diagram che descrive l'interazione tra una applicazione che voglia utilizzare il sistema IAM in oggetto e WSO2 stesso.



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



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")

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")

Autenticazione tramite eIDAS

Funzionalità in fase di sviluppo.

Endpoint esposti

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

Endpoint	Metodo	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:

Utilizzo	Endpoint
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

dove ***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:

Utilizzo	Endpoint
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
La password sarà fornita in fase di on-boarding

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

Creazione ed eliminazione di utenti

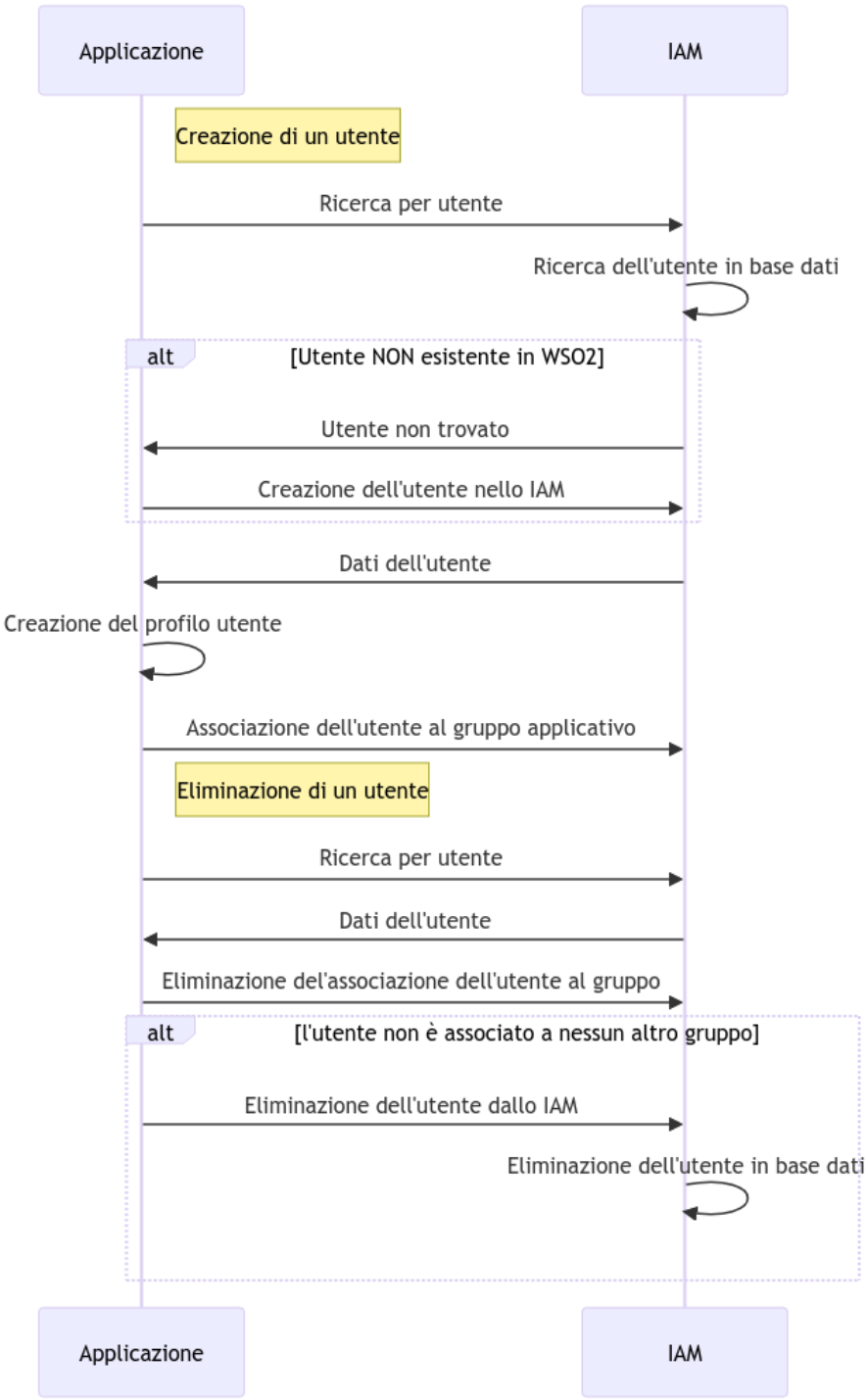
La responsabilità della corretta creazione ed eliminazione di una utenza da parte di un applicativo all'interno dello user store di WSO2 è a totale carico dell'applicativo stesso.
Poiché più applicazioni, all'interno dello stesso tenant, possono essere accedute dallo stesso utente e poiché WSO2 non ha indicazione alcuna su quali applicazioni profilino i diversi utenti della sua base dati, si è ritenuto opportune 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 avvenute) 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"
2. 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}
3. 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}


Applicazione
IAM
Creazione di un utente
Ricerca per utente
Ricerca dell'utente in base dati
alt
[Utente NON esistente in WSO2]
Utente non trovato
Creazione dell'utente nello IAM
Dati dell'utente
Creazione del profilo utente
Associazione dell'utente al gruppo applicativo
Eliminazione di un utente
Ricerca per utente
Dati dell'utente
Eliminazione del'associazione dell'utente al gruppo
alt
[l'utente non è associato a nessun altro gruppo]
Eliminazione dell'utente dallo IAM
Eliminazione dell'utente in base dati
Applicazione
IAM

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.