IAM

Specifiche integrazione modulo **I**dentity and **A**ccess **M**anagement

V 1.4

Indice generale

Indice delle figure

Indice delle tabelle

Acronimi

ID	Definizione
DB	**D**ata**B**ase
HW	**H**ard**W**are
IAM	**I**dentity **and** **A**ccess **M**anagement
IdP	**Id**entity **P**rovider
JWT	**J**SON **W**eb **T**oken
RP	**R**egione **P**uglia
SAML	**S**ecurity **A**ssertion **M**arkup **L**anguage
SP	**S**ervice **P**rovider
SPID	**S**istema **P**ubblico per l'**I**dentità **D**igitale
SSO	**S**ingle **S**ign-**O**n
SW	**S**oft**W**are
VM	**V**irtual **M**achine
WSO2	**W**eb **S**ervice **O**xygen **2**
WSO2 IS	**W**eb **S**ervice **O**xygen **2** **I**dentity **S**erver

1 Obiettivo

Il documento ha l'obiettivo di indicare le specifiche di integrazione che dovranno essere seguite dalle applicazioni che vogliono federarsi con la piattaforma IAM Puglia.
IAM è un gateway basato sulla piattaforma WSO2 IM che implementa tutte le modalità di accesso previste dal CAD:

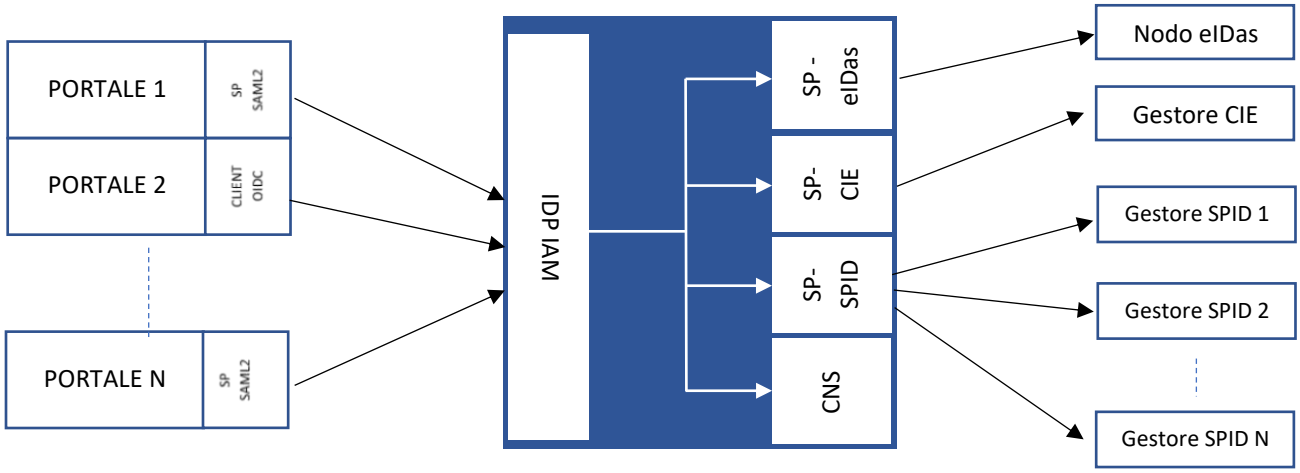

Figura 1: architettura IAM

Un applicativo (portale web o app mobile) si può interfacciare con IAM tramite SAML 2 o OpenId Connect.
Ogni portale di servizio implementa un client (SP SAML 2 o Client OIDC) che comunica con la componente IDP dell'IAM; a sua volta, l'IAM si presenta come Service Provider verso il mondo SPID/CIE/eIDas, implementa anche la funzionalità di interfacciamento tramite CNS e permette, con opportune configurazioni, un login tramite un repository di utenti pre-esistente..

Le applicazioni federate usufruiscono dei vantaggi offerti della piattaforma:

- Utilizzo di protocolli standard per la federazione
- Utilizzo di tutte le modalità di autenticazione previste dal CAD (SPID/CIE/CNS/eIDas)
- Disaccoppiamento rispetto alle modalità di autenticazione previste dal CAD: le eventuali modifiche alle regole tecniche hanno un impatto nullo o molto limitato sugli applicativi federati.
- Utilizzo della modalità username/password per utenti di back-office o non previsti dal CAD
- Integrazione di repository di utenti esistenti in diversi formati (ldap, active directory, database etc)
- Single Sign On: una volta inserita la password, non è più necessario autenticarsi su altri portali federati durante la sessione di lavoro
- Multi-tenancy: totale isolamento di domini applicativi
- Adaptive Login: possibilità di creare script da lanciare dopo il login, ad esempio per rafforzare la sicurezza e bloccare comportamenti anomali

2 Protocolli per la federazione

Il sistema supporta i seguenti protocolli di SSO:

- **SAML2**: per applicazioni web classiche
- **Oauth2/OpenID** JWT Bearer Tokens: per applicazioni mobile

Nelle sezioni seguenti andremo specificheremo le attività/configurazioni necessarie per una corretta integrazione.

2.1. SAML2

Security **A**ssertion **M**arkup **L**anguage (SAML) è un formato di dati basato su XML per lo scambio di dati di autenticazione un provider di identità e un fornitore di servizi.
Nelle specifiche SAML sono definiti tre ruoli principali:

- **Principal**: questo è in genere l'utente che tenta di accedere a una risorsa protetta
- **Identity Provider**: un provider di identità (IdP) è responsabile per l'autenticazione degli utenti e l'emissione di asserzioni che includono decisioni di autenticazione / autorizzazione e attributi dell'utente.
- **Service Provider**: un Service Provider (SP) consuma le asserzioni emesse dall'identy provider e fornisce servizi al principal.

In generale, utilizzando il protocollo SAML occorre preventivamente instaurare una "trust chain" tra SP e IDP; questo viene fatto tramite uno scambio preliminare di informazioni, ossia tramite lo scambio di *metadata*.
Un *metadata* è un file xml che contiene informazioni essenziali per l'identificazione degli attori coinvolti nella federazione e per la securizzazione del processo di autenticazione.

All'interno di questo file è necessario specificare:

- **Entity ID**: ID univoco rappresentante l'applicativo per il quale si presenta il metadata.xml
- **Certificati criptografici**: i certificati X509 in formato base64 che servono per firmare e criptare le request, le response e le asserzioni SAM
- **Endpoint del protocollo (bindings e locations):** le URL da chiamare durante lo scambio delle asserzioni e le modalità di binding supportate (POST, REDIRECT, SOAP etc)

Lo scenario di utilizzo principale coperto da SAML è l'utente che richiede l'accesso alla risorsa protetta. Quindi il Service Provider, utilizzando SAML, comunica con l'identity provider per ottenere l'assertion SAML che descrive l'identità dell'utente. Il service provider prende la decisione sul controllo degli accessi, in base a questa assertion.
Il flusso descritto è rappresentato nella figura seguente:

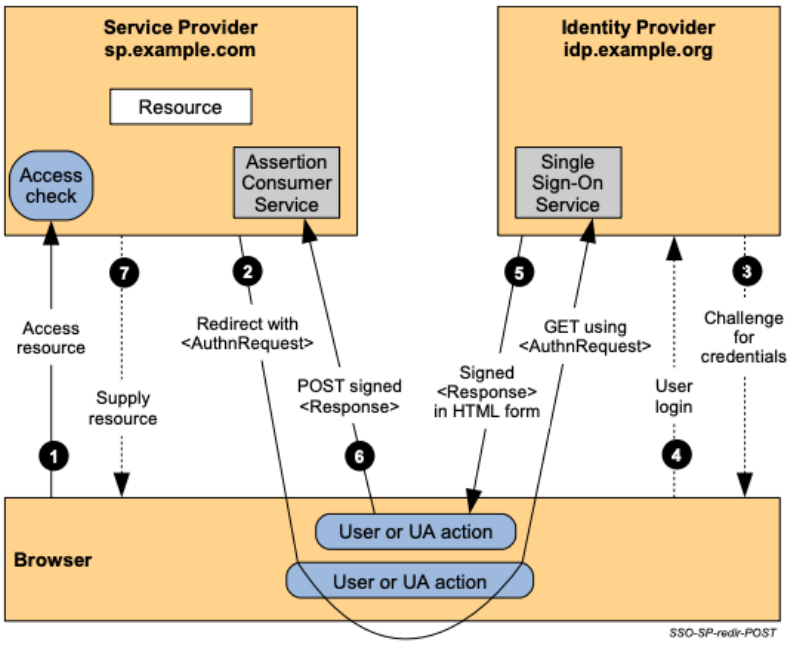

Figura 2: processo di autenticazione SP initiated HTTP-POST

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

1) l'utente navigando con il suo browser richiede l'accesso ad una risorsa protetta
2) Il SP invia una authentication request all'IDP federato, tramite il browser (User Agent)
3) L'IDP effettua la procedura di autenticazione; viene presentata all'utente la schermata di richiesta delle credenziali
4) L'utente inserisce le credenziali
5) L'IDP invia una response SAML in un html form al browser (User Agent)
6) Il browser ridireziona la response al SP
7) Il SP autorizza l'utente all'accesso alla risorsa.

Il protocollo SAML prevede anche altri profili di utilizzo, ma per limitare l'impatto delle modifiche sugli applicativi esistenti che hanno già implementato l'integrazione con SPID, per l'integrazione con IAM è previsto soltanto il profilo *"Web browser SSO"* con scenario *SP-initiated* e *Redirect/POST Bindings*.

2.1.1 Attributi SAML

Nella sezione seguente verranno descritti gli attributi che vengono restituiti da IAM a valle di una autenticazione avvenuta con successo. Nella tabella seguente verranno elencati gli attributi che possono essere presenti nella SAML response.
Per limitare l'impatto con le applicazioni già integrate con SPID, si usano gli stessi nomi e formati previsti dalle regole tecniche a cui si rimanda per i dettagli[1].

Si riporta qui per comodità l'elenco degli attributi e se sono disponibili nelle varie modalità di accesso.
Le ultime tre colonne indicano i 3 set di attributi disponibili; ogni service provider può esser configurato per utilizzare uno di questi set. In generale i set *minimo e esteso* sono da utilizzare per l'accesso ai cittadini, mentre quello *completo* è da utilizzare per gli accessi aziendali.

Attributo	Nome Attributo	Disponibile con				Set di attributi		
		SPID	CIE	CNS	EIDAS	Minimo	Esteso	Completo
Codice identificativo	spidCode	X			X* ***	X	X	X
Nome	name	X	X	X	X*	X	X	X
Cognome	familyName	X	X	X	X*	X	X	X
Luogo di nascita	placeOfBirth	X			X**		X	X
Provincia di Nascita	countyOfBirth	X					X	X
Data di nascita	dateOfBirth	X	X		X*	X	X	X
Sesso	gender	X			X**		X	X
Ragione o denominazione sociale	companyName	X			X***			X
Sede legale	registeredOffice	X			X****			X
Codice fiscale	fiscalNumber	X	X	X		X	X	X
Partita IVA	ivaCode	X			X****			X
Documento identità	idCard	X					X	X
Numero di telefono mobile	mobilePhone	X					X	X
Indirizzo posta elettronica	email	X					X	X
Domicilio fisico	address	X			X**		X	X
Domicilio digitale	digitalAddress	X					X	X

obbligatorio; **opzionale ; * obbligatorio per persone giuridiche; **** opzionale per persone giuridiche*

Tabella 1: Mappatura attributi SPID - attributi SAML

Tutti gli attributi sono stringhe testuali.
Il campo dateOfBirth è nel formato *yyyy-mm-dd*
Gli attributi restituiti a seguito di un login SPID dipendono dal set di attributi scelto dal SP.

[1] https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/attributi.html

I dati inclusi nei set di attributi descritti verranno restituiti a seguito del login se disponibili nella modalità di login scelta dall'utente; ad esempio la data di nascita, sebbene inclusa in tutti i set di attributi, non verrà restituita in caso di autenticazione con CNS.

2.1.2 Metadata SAML Request, SAML Response

In questa sezione verranno mostrati degli esempi di metadata, request e response SAML.
Qui https://samlecho.regione.puglia.it/applicazione-mock/ è disponibile un'applicazione demo conforme a quanto descritto di seguito.

2.1.2.1 Esempio di metadata

Nei metadata devono essere indicati:
entity_ID nel formato URI; per convenzione si può indicare la url del portale da integrare
Assertion Consumer Service: l'elenco degli endpoint SAML, con i relativi binding; deve essere presente almeno il binding HTTP-POST
Single Logout Service URL: le URL per il logout con i relativi binding; deve essere presente almeno il binding HTTP-POST
certificati di firma e criptazione di request e asserzioni. I certificati devono utilizzare l'algoritmo di hashing RSA-SHA256 o RSA-SHA512 e chiavi RSA con lunghezza non inferionre a 2048 bit.

Inoltre devono essere presenti gli attributi **AuthnRequestsSigned="true"** e **WantAssertionsSigned="true"** per accettare soltanto request e asserzioni firmate.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_b5b4d4f770af5db2c7f4aba2759728508b277b4f" entityID="ENTITY_ID">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#_b5b4d4f770af5db2c7f4aba2759728508b277b4f">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>o9cb+dE+Fp5vquP8/fkH1GqfFl4qnWBL+fF96ZoSLrE=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>UlAZ95zvNQ+qoflQptlB8olx2ZhnCawesGO7hBPNlZwLxoEi1FSmeVvVNA1W+zuC
.....
.....
Y3mejPLKGgo7AkCMzrWP0XZ9/31dIipjeI7VUfp3+CIlFNzFxN4IyY7D4VJHieMT</ds:SignatureValue>
<ds:KeyInfo><ds:KeyName>spid-
test.novalocal</ds:KeyName><ds:X509Data><ds:X509SubjectName>mySN</ds:X509SubjectName><ds:X509Certificat
e>MIIEADCCAmigAwIBAgIJAI3/WyEEdRcsMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
.....
.....
/wfk/61xQkUmCp/4KkSmjRD47Fo=
</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature>

<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>test</ds:KeyName>
        <ds:X509Data>
          <ds:X509SubjectName>mycertName</ds:X509SubjectName>
```

```
          <ds:X509Certificate>MIIEADCCAmigAwIBAgIJAI3/WyEEdRcsMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
.....
.....

/wfk/61xQkUmCp/4KkSmjRD47Fo=
</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>test</ds:KeyName>
        <ds:X509Data>
          <ds:X509SubjectName>mycertName</ds:X509SubjectName>
          <ds:X509Certificate>MIIEADCCAmigAwIBAgIJAI3/WyEEdRcsMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
.....
.....

/wfk/61xQkUmCp/4KkSmjRD47Fo=
</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>

    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://MY_SLO_URL"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://MY_ACS_URL" index="1"/>
  </md:SPSSODescriptor></md:EntityDescriptor>
```

2.1.2.2 Esempio SAML Request

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest
    AssertionConsumerServiceURL="https://MY_ACS_URL"
    Destination="https://login-test.regione.puglia.it/samlsso" ForceAuthn="false"
    ID="a11hh3g23c3bcb2d34he7ha49db5fga" IsPassive="false" IssueInstant="2021-02-08T15:00:47.293Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0"
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">ENTITY_ID</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256"/>
            <ds:Reference URI="#a11hh3g23c3bcb2d34he7ha49db5fga">
                <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
                <ds:DigestValue>K5Zoe/6sKFAp+4JFvpQGOujBJcM=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>RnJbw+t1e2hHLd5HgtsJp/9DY41wXtf6TCenV2DMkciVbp7f6FV3Ue+MfI94xoW8iPvDIevE……
iHGzg2rKCA82rkeZh7CuJ7IdSf+Za/KKAbNBYC4t2/G2EU3+PoWme+uvHO/QmWpcI=</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIHRzCCBi+gAwIBAgIMc0NgaIMc65RoWA8CMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
……
W7UkkGvBoHh9uNnh2TOA8XV6f6fMl++QnYUnrlc/pvf73HI4x4LJasuRpA==</ds:X509Certificate>

<ds:X509Certificate>MIIETTCCAzWgAwIBAgILBAAAAAABRE7wNjEwDQYJKoZIhvcNAQELBQAwVzELMAkGA1UEBhMCQkUx
                    ……
                     nl7OedSyps9AsUSoPocZXun4IRZZUw==</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</saml2p:AuthnRequest>
```

Da osservare che l'attributo ***ForceAuthn="false"*** sta ad indicare che l'applicazione non richiede la forzatura della richiesta di login ma utilizza i dati di login eventualmente presenti in sessione da una autenticazione precedente: è il parametro che indica che è attivato il Single Sign On per l'applicazione. Il valore "true", al contrario, indica che il SSO non è supportato.

2.1.2.3 Esempio SAML Response

L'applicazione invia allo IAM una SAML Request di tal tipo:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://MY_ACS_URL"
    ID="_633afd3c850e9c810e4669e3dd6f8b02" InResponseTo="a11hh3g23c3bcb2d34he7ha49db5fga"
    IssueInstant="2021-02-08T15:00:52.354Z" Version="2.0"
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://login-
test.regione.puglia.it/</saml2:Issuer>
    <saml2p:Status><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status>
    <saml2:Assertion ID="_49589b966337020551dd550a7f5736f4" IssueInstant="2021-02-08T15:00:52.354Z"
        Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://login-
test.regione.puglia.it/</saml2:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
                <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256"/>
                <Reference URI="#_49589b966337020551dd550a7f5736f4">
                    <Transforms>
                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"><ec:InclusiveNamespaces PrefixList="xsd" xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"/></Transform>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
                    <DigestValue>lrxfR4GPbeCjJ8y/X7gdmANu5QY=</DigestValue>
                </Reference>
            </SignedInfo>
            <SignatureValue>
                vMLW4Sc5ttbeBEW4S4v9EpiL5Liq8H6dQn4xUG1609MsRShgpId44lsyBht4VRVhUMKQkw+TkiW7
……
                w8WZNKx4F89eMZVwPn0EILi4IfFFh4yh57VG9KPq/jEfPVkqs3cJvxphdKkZNqWLvzS6sFIS5IQ=
            </SignatureValue>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>

<ds:X509Certificate>MIIHRzCCBi+gAwIBAgIMc0NgaIMc65RoWA8CMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
……
……
W7UkkGvBoHh9uNnh2TOA8XV6f6fMl++QnYUnrlc/pvf73HI4x4LJasuRpA==</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </Signature>
        <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">esempioSaml</saml2:NameID>
            <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml2:SubjectConfirmationData
InResponseTo="a11hh3g23c3bcb2d34he7ha49db5fga"
                NotOnOrAfter="2021-02-08T15:05:52.354Z"
                Recipient="https://MY_ACS_URL"></saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2021-02-08T15:00:52.354Z" NotOnOrAfter="2021-02-08T15:05:52.354Z">
            <saml2:AudienceRestriction>
                <saml2:Audience> ENTITY_ID</saml2:Audience>
```

```
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2021-02-08T14:53:37.732Z"
            SessionIndex="b98a0ebe-a283-48b2-8dc1-d706e18377fd">
            <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml2:AuthnContextClassRef
>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute Name="ivaCode" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">12345678909</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="placeOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">Bari</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">DOMICILIO FISICO</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="gender" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">M</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="idCard" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">TEST IDENTI</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="companyName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">Denominazione sociale</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="spidCode" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">5055a5b2-c078-11ea-b3de-0242ac130004</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="dateOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">1980-10-10</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="mobilePhone" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">2423423423</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="familyName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">Saml</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="digitalAddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">TEST@PEC.IT</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
```

```
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">Esempio</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="countyOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">BA</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="registeredOffice"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">Bari Legale</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="fiscalNumber" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">MMRNNN76R22Y658J</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">esempioSaml@test.it</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="expirationDate"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">2030-10-10</saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

Come si vede dalla response precedente, lo IAM restituisce tutti gli attributi elencati nella **obbligatorio; **opzionale ; *** obbligatorio per persone giuridiche; **** opzionale per persone giuridiche*
Tabella 1
Sarà compito dell'applicativo target gestire opportunamente gli attributi restituiti.

2.1.3 Integrazione di repository utenti esistenti

IAM offre la possibilità di login tramite username e password. I dati degli utenti possono risiedere nello user store primario di wso2 (interno alla piattaforma) oppure può essere contenuti in uno o più user store secondari, esterni alla piattaforma e integrati con essa.
È possibile configurare più di uno user store, nei formati più comunemente usati, tra cui ldap, active direcory, DB SQL.
Se necessario, quindi, un'applicazione può essere integrata nella piattaforma insieme agli utenti esistenti in maniera trasparente agli utenti stessi, in modo che essi possano continuare ad usare le proprie credenziali.
In questo caso, *in generale* il provisioning degli utenti resta responsabilità del gestore del servizio applicativo, che continuerà ad utilizzare le proprie procedure di gestione degli utenti (registraizone, recupero password, controlli sulla sicurezza delle password etc).
L'integrazione di user stores esterni va analizzata e implementata caso per caso.

2.1.4 Procedura integrazione IAM via SAML

La procedura di integrazione tecnica consiste nel compilare e spedire l'Allegato A in cui vengono specificate le informazioni amministrative dell'ente e del fornitore che implementa l'integrazione e i dati tecnici per poter integrare i sistemi.
Il fornitore del servizio dovrà implementare un Service Provider SAML2 che possa inviare request conformi e riesca a elaborare le response conformi a quanto descritto nei paragrafi precedenti

E' disponibile un ambiente di test/collaudo di IAM in cui effettuare tutte le prove di integrazione.

I metadata di IAM di test dall'URL https://www.rupar.puglia.it/iam/login-test.regione.puglia.it.xml

L'ambiente di test di IAM è integrato con il gestore SPID di test rilasciato da AGID; questo supporta il solo livello 1.

A seguito dei test si potrà effettuare l'integrazione con l'ambiente di esercizio; i metadata di IAM di esercizio sono scaricabili da https://login.regione.puglia.it/identity/metadata/saml2

2.2. OpenID Connect

OpenID Connect è un protocollo di autenticazione/autorizzazione che è diventato uno standard di riferimento per l'implementazione del Single Sign On in internet.
Si tratta molto brevemente di un protocollo che invia token di identità in formato JSON (JSON Web Token o JWT) tramite protocollo OAuth 2.0, ormai protocollo di riferimento per le applicazioni mobili e anche per il web.
JWT è uno standard aperto (RFC 7519) che definisce un modo compatto e autonomo per trasmettere in modo sicuro le informazioni tra le parti in formato JSON.
L'informazione trasmessa è firmata digitalmente o usando una funzione di hash (con l'algoritmo HMAC) oppure tramite una coppia di chiavi pubblica / privata usando RSA o ECDSA.
È possibile consultarele specifiche OAuth2 al seguente link https://tools.ietf.org/html/rfc6749

Oggigiorno lo scenario più comune per l'utilizzo di JWT è quello dell'autenticazione. Una volta che l'utente ha effettuato l'accesso, ogni richiesta successiva includerà il JWT in uno specifico header HTTP. A causa del suo piccolo overhead e della sua capacità di essere facilmente utilizzato in diversi domini i bearer token JWT sono largamente utilizzati in applicazioni mobile e di tipo SPA.
Una volta ottenuto il token JWT, questo, per ogni HTTP request, è inserito nell'header HTTP chiamato "*Authorization*".
L'immagine seguente schematizza il diagramma di interazione per l'autenticazione tramite token JWT

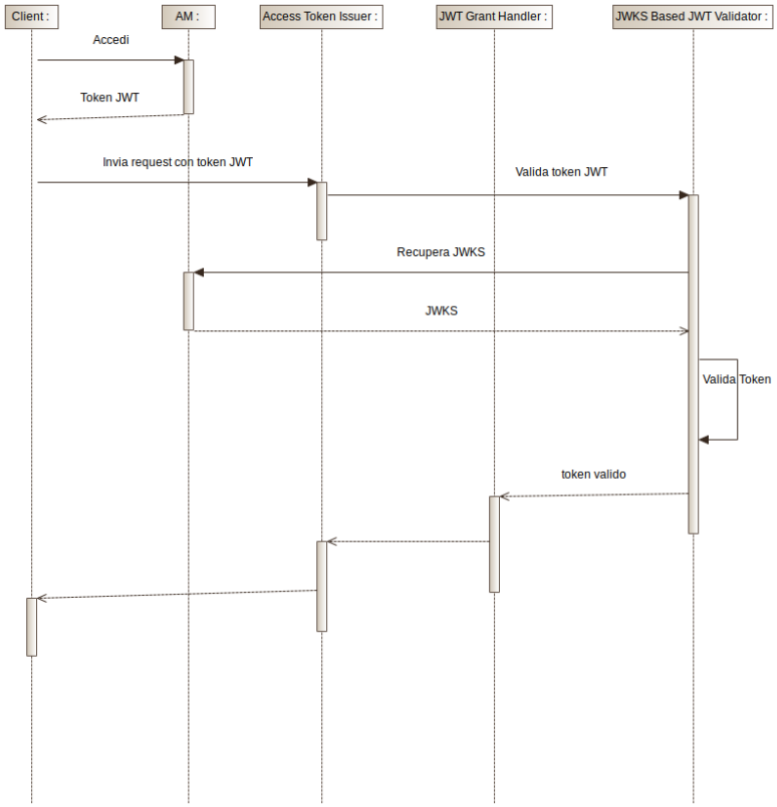

Figura 3: Autenticazione JWT Bearer token

Maggiori dettagli si possono trovare sul sito di riferimento https://openid.net/
Una volta ottenuto il token JWT, questo deve essere inserito nell'header HTTP di ogni chiamata verso le risorse protette.
Per l'autenticazione con lo IAM regionale verranno supportati i seguenti oauth2 authorization grant:

- authorization code con PCKE: utilizzato per integrare applicazioni web e app mobile
- client credentials: utilizzato per integrare eventuali sistemi di background (e.g. processi batch etc...)

Per dettagli sui grant oauth supportati si può far riferimento ai seguenti link:

- authorization code: https://tools.ietf.org/html/rfc6749#section-1.3.1

- client credentials: https://tools.ietf.org/html/rfc6749#section-1.3.4

In entrambi i casi è necessario recuperare un token JWT per poter poi accedere alle risorse protette di un eventuale sistema.
Ottenuto il token JWT è necessario aggiungerlo nel header HTTP Authorization come mostrato di seguito:
“
Authorization: Bearer valore_token
”
Affinché questo scenario sia configurato correttamente, l’applicazione deve indicare:

- post login URL: URL dove redirigere l’utente quando l’autenticazione va a buon fine
- post logout URL: URL dove redirigere l’utente quando il logout va a buon fine
- authorization grant: grant utilizzato per lo scenario di autenticazione. In particolare:
  - scenario authorization code: l’authorization grant da usare è **authorization_code**
  - scenario client credentials: l’authorization grant da usare è **client_credentials**
- scope: gli scope da richiedere sono **openid profile email api**

Lo IAM espone un openid well known endpoint che riporta tutte le informazioni necessarie utili alla federazione dei verticali via OAuth2/OpenID.
Gli URL sono i seguenti:

- ambiente test: https://login-test.regione.puglia.it/oauth2/token/.well-known/openid-configuration
- ambiente produzione: https://login.regione.puglia.it/oauth2/token/.well-known/openid-configuration

All’applicazione, invece, l’IdP fornirà:

- clientId: ID univioco del client che viene utilizzato per la generazione dei token JWT
- secretKey: chiave segreta per l’autenticazione.

Una volta scambiate le informazioni indicate, utilizzando il protocollo Oauth2 di tipo implicito, viene generato un token JWT in formato Base64.
Come detto in precedenza, ottenuto il token JWT è necessario passarlo come header HTTP per ogni richiesta. In sintesi in ogni chiamata HTTP deve essere presente l’header “`Authorization: Bearer`” che riporta il token JWT