

ROMA



Integrazione applicativa con il servizio di Identity and Access Management

Specifiche tecniche per l'integrazione di applicazioni

Edizione 11 del 21/4/2022

Le informazioni contenute in questo documento sono di esclusiva proprietà del RTI Fastweb-Leonardo. Questo documento non può essere riprodotto per intero o in parte senza il consenso scritto del RTI.

Integrazione applicativa con il servizio di Identity and Access Management

Specifiche tecniche per l'integrazione di applicazioni

Versione 11 – 20220421

Compilazione	Marco Benucci, Marco Liverani, Enrico Pili
Revisione	Enrico Pili, Marco Liverani
Approvazione	Mauro Tosca
Distribuzione	RTI Fastweb – Leonardo, Roma Capitale, Fornitori Roma Capitale

Versione Documento #	Data di Approvazione	Modificato da	Modifiche
1	3/5/2016	RTI	Prima stesura
2	27/7/2016	RTI	Modifiche all'elenco delle variabili header
3	5/9/2016	RTI	Aggiunta della sez. 3.3 per utenze SPID
4	6/10/2016	RTI	Modifica alla sez. 3.3 per utenze SPID
5	5/12/2016	RTI	Aggiunta sez. 2.2, aggiunto Capitolo 4
6	16/12/2016	RTI	Modifiche al Capitolo 4
7	26/4/2017	RTI	Modifiche alla sez. 3.2 (variabili header)
8	4/7/2017	RTI	Aggiunta la sez. 3.4 (codifica dei caratteri)
9	3/5/2019	RTI	Aggiunta la sez. 3.3 (dati persona giuridica)
10	23/6/2020	RTI	Modificata sez. 3.3 (dati persona non giuridica o delegata). Modifica sezione 3.2 (aggiunta la provincia di nascita)
11	21/4/2022	RTI	Integrazione mediante OpenID Connector (OIDC)

Indice degli argomenti

1	Introduzione	3
1.1	Scopo del documento	3
1.2	Ambito	3
1.3	Definizioni e acronimi	3
1.4	Organizzazione del documento	4
2	Architettura logica del servizio IAA	5
2.1	Componenti del servizio IAA	5
2.2	Configurazione dell'infrastruttura applicativa	6
2.3	Processo di Autenticazione ed Autorizzazione	7
2.4	Autenticazione federata	8
3	Specifiche tecniche per l'integrazione	10
3.1	Il processo di autenticazione e autorizzazione	10
3.2	Il passaggio dei valori da IAM all'applicazione	11
3.3	Informazioni sulla persona giuridica rappresentata dalla persona fisica o delegata	14
3.4	Autenticazione con SPID	15
3.5	Codifica dei caratteri	16
3.5.1	JEE con Java 6 e 7	16
3.5.2	JEE con Java 8	17
3.5.3	Microsoft .net – C#	17
3.6	Autenticazione con OIDC	17
3.7	Claim e scope supportati	17
3.7.1	Specifiche tecniche per l'integrazione	18
3.7.2	Il processo di autenticazione e richiesta degli attributi utente	18
4	Processo di configurazione degli ambienti di esercizio e pre-esercizio	21
4.1	Informazioni necessarie per la configurazione degli ambienti Portale e IAM	21
4.2	Riferimenti dei gruppi di gestione	22

1 Introduzione

Il presente documento fornisce le specifiche per l'integrazione di applicazioni web based di Roma Capitale con i servizi di autenticazione e autorizzazione degli utenti offerti dall'infrastruttura di Identity and Access Management integrata con il Portale Istituzionale.

1.1 Scopo del documento

Lo scopo del documento è quello di fornire indicazioni tecniche destinate ai progettisti applicativi, agli architetti software e agli sviluppatori, per progettare e realizzare l'integrazione software tra le applicazioni web based realizzate per Roma Capitale e il sistema di Identity and Access Management (IAM). Quest'ultimo si occupa della registrazione e della gestione del ciclo di vita delle credenziali attribuite agli utenti (interni ed esterni) che sono abilitati ad operare sulle applicazioni on-line di Roma Capitale; il sistema IAM offre anche il servizio di autenticazione e autorizzazione degli utenti che deve essere sfruttato dalle applicazioni al fine garantire il corretto utilizzo delle credenziali di autenticazione e delle autorizzazioni rilasciate dai responsabili del Dipartimento Trasformazione Digitale (DTD).

1.2 Ambito

Il documento rappresenta uno dei deliverable rilasciati nell'ambito dell'attività di presa in carico del servizio IAA (Identificazione, Autenticazione e Autorizzazione) realizzato per Roma Capitale. In questo ambito viene predisposto un nuovo sistema di Identity and Access Management per l'erogazione del servizio IAA e questo documento fornisce delle specifiche tecniche per l'integrazione di applicazioni esterne con i servizi offerti dalla nuova piattaforma IAM.

1.3 Definizioni e acronimi

Nel presente documento sono utilizzate sigle, acronimi e termini tecnici descritti nella seguente tabella.

Definizione	Descrizione
AD	Microsoft Active Directory
AM	Sistema di Web Access Management (componente del sistema IAM)
CRM	Customer Relationship Management
DB	Data base
DBMS	Data Base Management System
DS	Directory Server
DTD	Dipartimento Trasformazione Digitale di Roma Capitale

Definizione	Descrizione
IAA	Sistema informatico che eroga i servizi di identificazione, autenticazione e autorizzazione degli utenti del sistema informativo di Roma Capitale
IAM	Sistema informatico di Identity and Access Management
IDM	Sistema informatico di Identity Management (componente del sistema IAM)
IF	Identity Federation
LDAP	Lightweight Directory Access Protocol
OAM	OpenAM
OIDC	OpenID Connect
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SPID	Sistema Pubblico di Identificazione Digitale (http://www.spid.gov.it)
SSO	Single sign-on
UTF-8	Unicode Transformation Format, 8 bit: codifica di caratteri Unicode

Tabella 1: Definizioni e acronimi

1.4 Organizzazione del documento

Il documento è articolato su quattro capitoli, oltre questo breve capitolo introduttivo.

Nel Capitolo 2 viene presentata l'architettura logica del sistema IAM che eroga i servizi di registrazione e gestione delle credenziali e delle autorizzazioni degli utenti, oltre al servizio di autenticazione e di autorizzazione per le applicazioni on-line (web application) di Roma Capitale.

Nel Capitolo 3 vengono proposte le specifiche tecniche per l'integrazione del servizio di controllo degli accessi (autenticazione e autorizzazione) su una web application rilasciata sul sistema informativo di Roma Capitale (servizi on-line offerti al cittadino sul Portale istituzionale o applicazioni web interne).

Nel Capitolo 4 viene descritto il processo in base al quale può essere richiesta ed effettuata l'integrazione di un nuovo servizio applicativo con il sistema IAM.

2 Architettura logica del servizio IAA

In questo brevissimo capitolo viene presentata e descritta l'architettura logica del servizio IAA e lo scenario di integrazione specificato in dettaglio nei capitoli seguenti.

2.1 Componenti del servizio IAA

Il servizio IAA viene offerto attraverso un sistema IAM composto dalle seguenti componenti applicative:

- **Sistema Identity Management:** è la componente che gestisce il ciclo di vita delle identità digitali degli utenti (interni ed esterni) del sistema informativo di Roma Capitale; ciascuna identità è composta da dati identificativi e anagrafici dell'utente e dai dati che caratterizzano le sue utenze sui sistemi informatici a cui è autorizzato ad accedere (username, profili autorizzativi, altre informazioni che qualificano l'utente);
- **Self-service management tools:** è il *front-end* web based reso disponibile agli utenti nell'area riservata del Portale istituzionale (la sezione "*Area riservata*") per accedere alle proprie informazioni e gestirle autonomamente (es.: cambio della password su tutti gli account assegnati agli utenti interni, modifica dei propri dati personali, ecc.);
- **Access Manager:** è la componente che offre i servizi di autenticazione e autorizzazione degli utenti e che gestisce le politiche di protezione delle applicazioni web based integrate con il sistema; svolge il ruolo di identity provider nel contesto di federazione con le applicazioni dei servizi on-line;
- **Web Policy Agent:** è la componente del sistema di controllo degli accessi e delle autorizzazioni che filtra tutte le richieste HTTP effettuate dagli utenti verso gli application server, applicando le policy di protezione delle diverse URL protette dal sistema.
- **Sistemi di registrazione degli utenti:** form e procedure di registrazione di nuovi utenti interni (dipendenti e collaboratori di Roma Capitale) ed esterni (cittadini che intendono usufruire dei servizi on-line) disponibili sul Portale istituzionale.
- **Sistemi di gestione degli utenti:** componenti del sistema Identity Management con cui gli operatori abilitati possono compiere operazioni di identificazione/abilitazione di nuovi utenti, di abilitazione, disabilitazione, assegnazione e revoca di autorizzazioni, nell'ambito del processo di gestione del ciclo di vita delle credenziali assegnate agli utenti.

Il sistema di autenticazione (Access Manager) del sistema IAM è inoltre integrato con una componente esterna al sistema, denominata "**Traduttore-PG**", che svolge il ruolo di intermediario tra il sistema IAM e altre sorgenti informative autoritative. In particolare, interrogando la componente Traduttore-PG, il sistema IAM può associare l'utenza relativa alla persona fisica autenticata dal sistema, con una *Persona Giuridica* (impresa economica) per conto della quale l'utente ha un ruolo di rappresentanza.

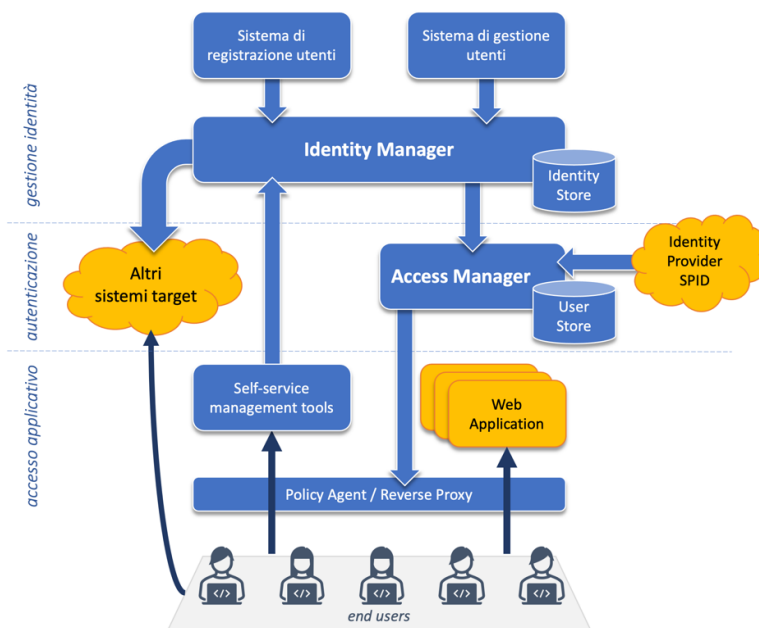


Figura 1: Architettura logica macroscopica del sistema IAM

Le informazioni relative agli utenti e alle loro autorizzazioni utilizzate da Access Manager sono gestite da Identity Manager e trasmesse sul Directory Server (*user store*) del sistema Access Manager attraverso procedure automatizzate di *provisioning*.

Le politiche di protezione sono basate sull'associazione di una URL (risorsa da proteggere, ad esempio l'area riservata di un'applicazione) ad uno schema di autenticazione e ad un profilo di autorizzazione.

2.2 Configurazione dell'infrastruttura applicativa

A livello macroscopico, l'infrastruttura applicativa di Roma Capitale può essere descritta come in Figura 2.

La comunicazione originata dal client (web browser) dell'utente esterno collegato alla rete Internet o dell'utente interno collegato alla rete interna di Roma Capitale, viene raccolto dal *reverse proxy* dell'infrastruttura di controllo accessi (sistema IAM).

Sulla base della URL richiesta viene stabilito dall'infrastruttura di front-end di IAM, se si tratta di una risorsa protetta, su cui è richiesta l'autenticazione e la successiva autorizzazione dell'utente, o se la risorsa è ad accesso pubblico/anonimo.

Nel primo caso viene eseguita una richiesta HTTP al reverse proxy posto di fronte all'infrastruttura degli application server.

Nel secondo caso viene prima autenticato l'utente e verificata la sua autorizzazione ad accedere alla risorsa richiesta; nel caso in cui l'utente abbia superato la fase di autenticazione e autorizzazione, viene eseguita una richiesta HTTP al reverse proxy dell'infrastruttura degli application server, dopo aver arricchito l'header della request HTTP con variabili header contenenti informazioni sulla virtual identity dell'utente che è stato autenticato (identificativo utente, nome, cognome, codice fiscale, indirizzo e-mail, ecc.).

La risposta alla request HTTP del proxy server dell'infrastruttura applicativa viene rigirata al reverse proxy dell'infrastruttura IAM che a sua volta la rigira al client dell'utente.

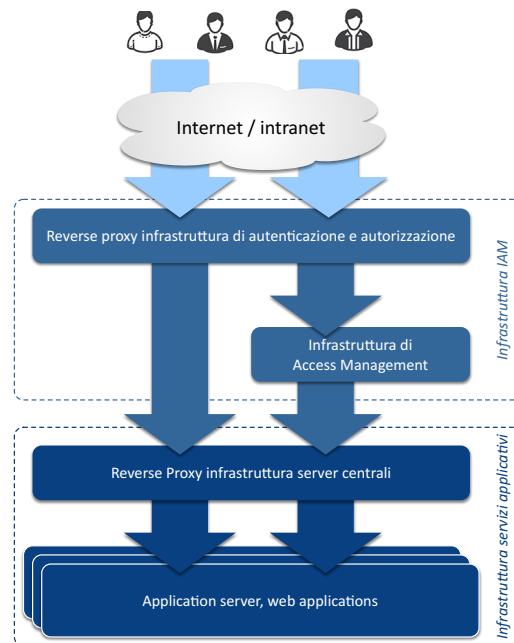


Figura 2: Schematizzazione macroscopica dell'infrastruttura applicativa

Nel Capitolo 4 vengono fornite le istruzioni per richiedere la configurazione delle componenti sopra descritte, negli ambienti di pre-produzione, adibiti al test e al collaudo delle applicazioni, e di produzione, dedicato all'erogazione dei servizi in esercizio.

2.3 Processo di Autenticazione ed Autorizzazione

Il sistema di Access Manager consente la gestione del processo di identificazione e di autorizzazione dell'utente alle applicazioni web presenti nel sistema informativo di Roma Capitale. Il sistema di Access Management è integrato, oltre che con la procedura informatica a cui fornisce il servizio di autenticazione ed autorizzazione dell'utente, anche con il sistema di Identity Management che determina le regole mediante cui sono concesse o gestite le autorizzazioni per ciascun utente del sistema informativo.

La comunicazione tra le applicazioni web e l'Access Manager, componente infrastrutturale che offre funzionalità di autenticazione e controllo degli accessi, avviene attraverso il componente Web Policy Agent, configurato in modalità di reverse proxy che filtra tutte le richieste eseguite dai client e destinate ad application server protetti dal sistema.

Ogni volta che viene richiesta una risorsa protetta da Access Manager, il componente Web Policy Manager, intercettando la richiesta HTTP inviata dal client (web browser) al server (web server), richiederà al sistema di Access Manager di autorizzare l'utente ad accedere a tale risorsa; nel caso in cui l'utente risulti anonimo o non possieda i privilegi necessari per accedere a tale risorsa, verrà automaticamente reindirizzato verso l'ambiente di autenticazione.

L'autenticazione dell'utente è un servizio implementato dal sistema Access Manager, completamente separato da ciascuna applicazione intranet. L'autenticazione può avvenire mediante diversi metodi (in gergo: schemi di autenticazione o *authentication schema*).

È importante sottolineare che la scelta della modalità di autenticazione è del tutto indipendente dall'applicazione e viene definita a livello di configurazione della "politica di autenticazione" sul sistema Access Manager per ogni specifica applicazione web. L'applicazione, infatti, otterrà in ogni caso le medesime informazioni relative alla sessione utente creata dal sistema di Access Management, indipendentemente dalla modalità con cui l'utente è stato riconosciuto dal sistema.

In Figura 1 sono riportate con un *sequence diagram*, le fasi di accesso ad una risorsa protetta da parte di un web browser, autenticazione dell'utente e richiesta successiva di una ulteriore risorsa web protetta.

L'applicazione web non implementa né le funzionalità di accesso e login, né le funzioni per la verifica dell'autorizzazione dell'utente ad accedere ad una specifica risorsa. Può invece ottenere dal sistema di Access Management delle informazioni aggiuntive che caratterizzano l'identità dell'utente connesso, attraverso la lettura di apposite *header variables* della sessione HTTP.

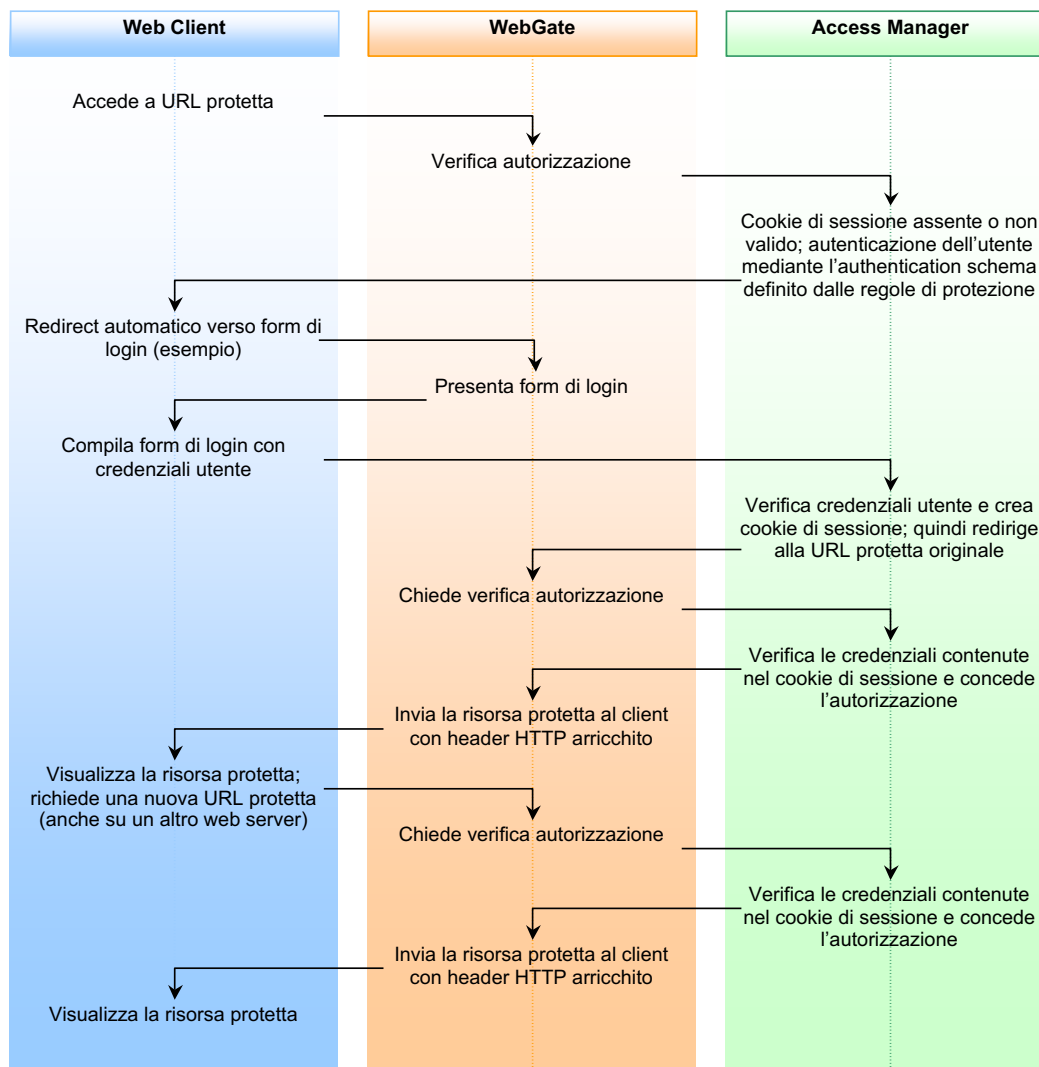


Figura 3: Processo di autenticazione e autorizzazione per una web application

2.4 Autenticazione federata

Il sistema IAM mette a disposizione altre due opzioni per l'integrazione di sistemi applicativi, attraverso tecniche di *identity federation* basate sul protocollo **SAML 2.0** o sul protocollo **OpenID Connect (OIDC)**.

Nel primo caso il componente Access Manager del sistema IAM svolge il ruolo di Identity Provider nei confronti dell'applicazione, che svolge il ruolo di Service Provider. L'autenticazione dell'utente e il successivo passaggio di attributi con informazioni sulla virtual identity dell'utente autenticato si svolge attraverso le asserzioni SAML.

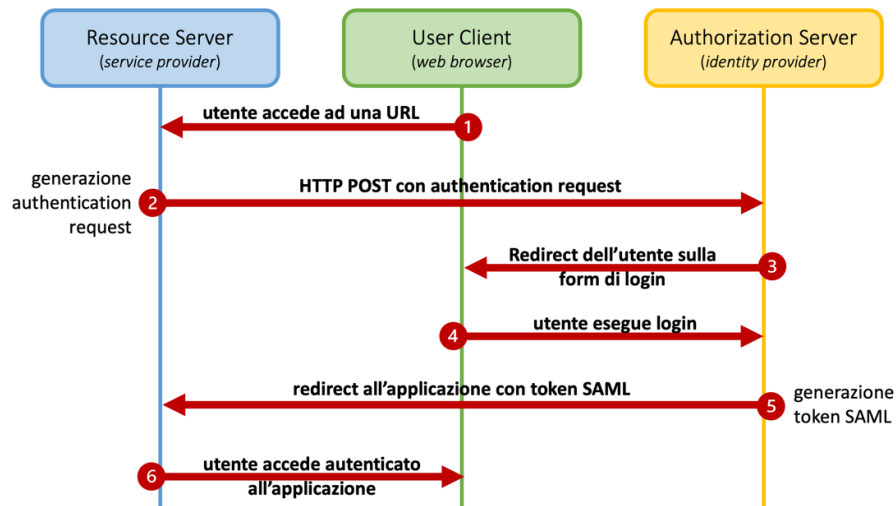


Figura 4: Sequence diagram della autenticazione di un utente con protocollo SAML

Il sistema IAM mette a disposizione anche la possibilità di autenticare gli utenti all'utilizzo della propria applicazione web, tramite il protocollo **OpenID Connect**, particolarmente adatto ad App Mobile e "single page application".

Questa tipologia di integrazione con il sistema IAM è sicuramente preferibile rispetto all'integrazione tramite web-agent, descritta nel capitolo precedente, ad esempio per applicazioni che richiedono numerosi accessi HTTP ai propri servizi di backend (come, ad esempio, le applicazioni basate su architettura a microservizi), senza che queste richieste debbano necessariamente essere arricchite con le header-variables descritte nel successivo Paragrafo 3.2.

Il sistema IAM supporta l'integrazione con flussi di autenticazione OIDC di tipo "authorization code", descritto ad alto livello dal sequence diagram riportato nella seguente **Figura 5**.

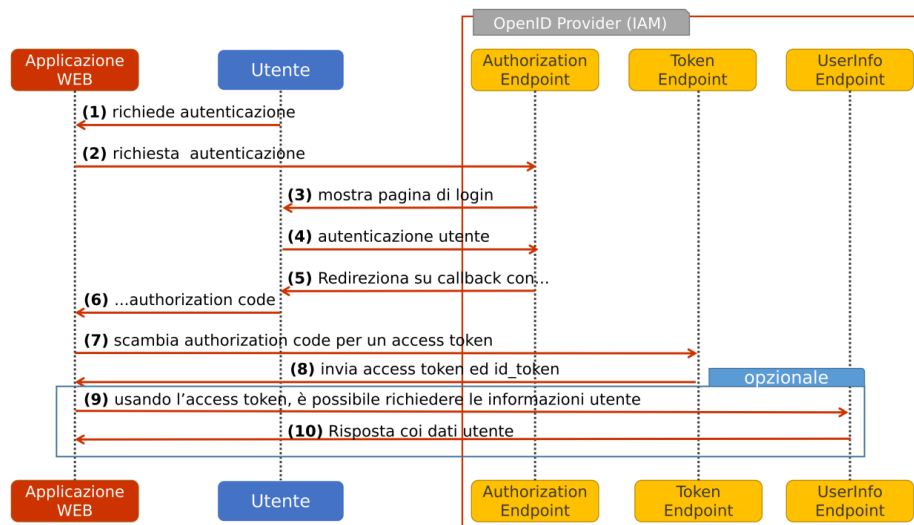


Figura 5: Sequence diagram della autenticazione di un utente con protocollo OIDC

3 Specifiche tecniche per l'integrazione

L'integrazione delle applicazioni viene realizzata proteggendo le URL delle applicazioni on-line, con una specifica configurazione di policy sul sistema Access Manager di Roma Capitale. Le applicazioni saranno raggiungibili non direttamente, ma attraverso la componente di *reverse proxy* dell'infrastruttura IAM.

Le applicazioni integrate con IAM beneficiano del servizio di autenticazione e autorizzazione degli utenti (che quindi non dovrà essere implementato dalle applicazioni stesse) e ricevono informazioni sull'utente autenticato e autorizzato ad accedere all'applicazione stessa, attraverso le variabili aggiunte dal sistema IAM nell'*header* HTTP. Di seguito sono indicate le modalità di dettaglio con cui l'applicazione può recepire le informazioni sull'utente autenticato.

È bene sin da ora sottolineare che con la parola "applicazioni" intendiamo applicazioni web-based il cui *engine* è un Application Server, che la modalità di interazione utente-applicazione avviene tramite il browser e il colloquio tra il browser e l'Application Server avviene tramite il protocollo HTTP/HTTPS.

3.1 Il processo di autenticazione e autorizzazione

Nel momento in cui l'utente accede a una applicazione identificata da una URL la richiesta viene intercettata dal componente *reverse proxy* di IAM, che si preoccupa di stabilire se l'utente che sta tentando l'accesso è autorizzato ad accedere all'applicazione stessa.

Se l'utente non risulta autenticato, ed è quindi impossibile controllarne le autorizzazioni, il *front-end* di *access management* si occupa di presentare all'utente la *form* di autenticazione e di verificare la validità delle credenziali inserite.

A fronte di un'autenticazione e autorizzazione avvenute con successo, vengono passate all'applicazione una serie di informazioni che sono gestite dal sistema Identity Management (che le avrà trasmesse in precedenza al sistema Access Manager mediante un'operazione di provisioning).

Le informazioni vengono rese disponibili tramite un insieme di variabili presenti nell'*header* HTTP. I dati che possono essere forniti all'applicazione corrispondono ai valori degli attributi dell'utente definiti sulla piattaforma IAM.

Nella figura seguente viene rappresentato il flusso di operazioni che consentono di autenticare e autorizzare un utente che richiede l'accesso ad una URL protetta da Access Manager.

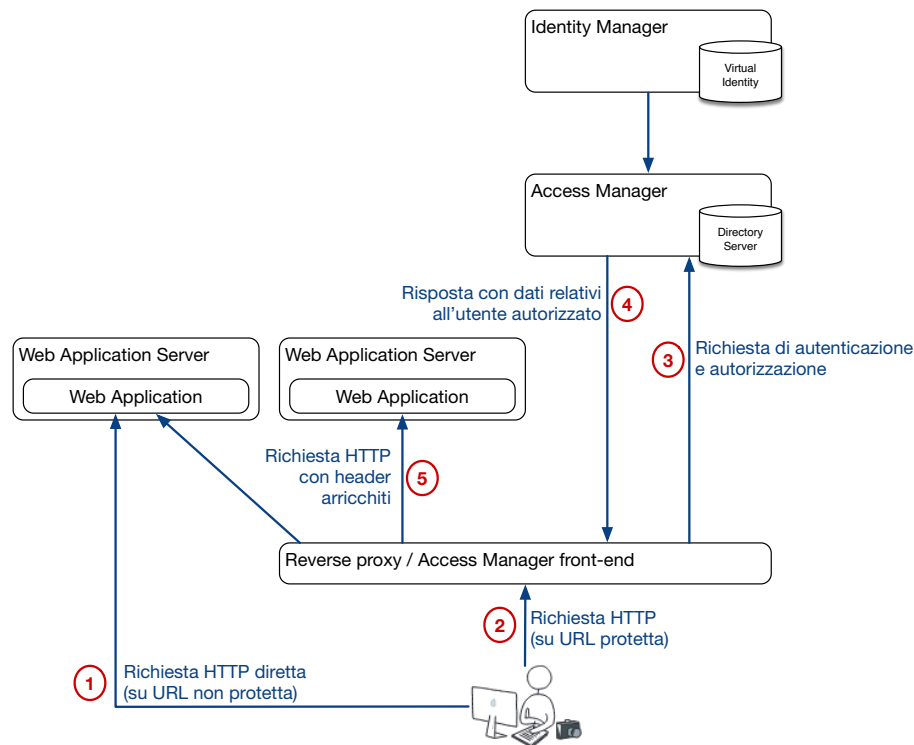


Figura 6: Flusso di comunicazione per l'autenticazione e l'autorizzazione

Facciamo riferimento alla **Figura 6**, descriviamo sinteticamente le singole interazioni:

1. Il browser dell'utente richiede l'accesso ad una URL non protetta dall'infrastruttura IAM; lo scambio avviene senza alcuna intermediazione da parte della piattaforma IAM e l'applicazione non riceve informazioni sull'utente.
2. Il browser dell'utente richiede l'accesso ad una URL protetta dall'infrastruttura IAM; la richiesta HTTP viene intercettata dalla componente di *front-end* del sistema IAM.
3. Se l'utente non è ancora autenticato, il *front-end* di Access Management presenta la *form* di autenticazione. Se l'utente è già autenticato, il sistema di Access Management non visualizza una *form* di autenticazione, ma verifica comunque l'autorizzazione dell'utente ad accedere alla URL richiesta.
4. Access Manager comunica l'esito dell'autenticazione e dell'autorizzazione dell'utente rispetto alla URL richiesta.
5. La richiesta correttamente autorizzata viene girata dal *reverse proxy* all'applicazione web; l'*header* HTTP della richiesta viene arricchito con le variabili contenenti le informazioni relative all'utente.

3.2 Il passaggio dei valori da IAM all'applicazione

Il passaggio all'applicazione web dei valori di autenticazione da IAM, gli attributi che caratterizzano l'identità virtuale (IV) dell'utente, avviene mediante l'arricchimento dell'*header* HTTP con un insieme di variabili (coppie chiave/valore). L'applicazione potrà quindi esaminare l'*header* HTTP della richiesta corrente per estrarre i valori ad essa necessari. L'infrastruttura IAM di Roma Capitale offre il servizio di autenticazione e autorizzazione in maniera del tutto indipendente dalla specifica tecnologia con cui viene realizzata l'applicazione web.

Ad esempio, supponendo che l'applicazione abbia bisogno di conoscere lo username dell'utente autenticato, potrà operare come segue (presentiamo la stessa istruzione usando diversi linguaggi di programmazione):

- ASP "classico"

```
Request.ServerVariables["IV-USER"]
```

- ASP.Net - VB.Net:

```
Request.Headers.Item("IV-USER")
```

oppure

```
Request.ServerVariables.Item("IV-USER")
```

- ASP.Net - C#:

```
Request.Headers["IV-USER"]
```

oppure

```
Request.ServerVariables["IV-USER"]
```

- Java:

```
request.getHeader("IV-USER")
```

Queste funzioni restituiscono una stringa di testo.

Al fine di limitare le incomprensioni riguardanti il passaggio di informazioni dall'Access Manager, in fase di sviluppo si consiglia di prevedere una pagina all'interno dell'applicazione, che stampi tutte le variabili contenute nell'header HTTP. Riportiamo un esempio con il codice di una pagina `ServerVariables.asp`:

```
<table>
  <%for each var in Request.ServerVariables %>
    <tr>
      <td>
        <%=var%>
      </td>
      <td>
        <%=Request.ServerVariables(var)%>
      </td>
    </tr>
  <%next%>
</table>
```

Nella tabella seguente sono riassunti gli attributi dell'identità virtuale dell'utente che possono essere resi disponibili dal componente di Access Management alle applicazioni web; tali informazioni sono disponibili come variabili presenti nell'header HTTP. Per ciascuna web application o per gruppi omogenei di applicazioni possono essere definite delle policy che rendano o meno disponibili alcune delle informazioni riportate nella tabella seguente. Per limitare la dimensione dell'header HTTP, le variabili disponibili per ciascuna applicazione dovranno essere ridotte a quelle strettamente indispensabili.

Variabile	Descrizione
iv-user	Username dell'utente autenticato
iv-portal-groups	Elenco dei gruppi LDAP a cui appartiene l'utente
iv-nome	Nome dell'utente
iv-cognome	Cognome dell'utente
iv-fullname	Nome e Cognome dell'utente
iv-sex	Genere dell'utente
iv-nascita-data	Data di nascita dell'utente
iv-nascita-comune	Denominazione estesa del comune di nascita dell'utente
iv-nascita-prov	Sigla della provincia di nascita
iv-nascita-nazione	Denominazione estesa del Paese di nascita

Variabile	Descrizione
iv-codfis	Codice fiscale dell'utente
iv-res-nazione	Dati relativi alla residenza dell'utente (denominazione della nazione)
iv-res-prov	Dati relativi alla residenza dell'utente (denominazione della provincia)
iv-res-comune	Dati relativi alla residenza dell'utente (denominazione del comune)
iv-res-via	Dati relativi alla residenza dell'utente (denominazione della strada)
iv-res-civico	Dati relativi alla residenza dell'utente (numero civico dell'indirizzo)
iv-res-int	Dati relativi alla residenza dell'utente (interno dell'abitazione)
iv-res-scala	Dati relativi alla residenza dell'utente (scala dell'abitazione)
iv-res-edificio	Dati relativi alla residenza dell'utente (edificio dell'abitazione)
iv-res-lotto	Dati relativi alla residenza dell'utente (lotto dell'abitazione)
iv-res-cap	Dati relativi alla residenza dell'utente (codice avviamento postale)
iv-dom-nazione	Dati relativi alla residenza dell'utente (denominazione della nazione)
iv-dom-prov	Dati relativi alla residenza dell'utente (denominazione della provincia)
iv-dom-comune	Dati relativi alla residenza dell'utente (denominazione del comune)
iv-dom-via	Dati relativi alla residenza dell'utente (denominazione della strada)
iv-dom-civico	Dati relativi alla residenza dell'utente (numero civico dell'indirizzo)
iv-dom-int	Dati relativi alla residenza dell'utente (interno dell'abitazione)
iv-dom-scala	Dati relativi alla residenza dell'utente (scala dell'abitazione)
iv-dom-edificio	Dati relativi alla residenza dell'utente (edificio dell'abitazione)
iv-dom-lotto	Dati relativi alla residenza dell'utente (lotto dell'abitazione)
iv-dom-cap	Dati relativi alla residenza dell'utente (codice avviamento postale)
iv-email	Indirizzo e-mail dell'utente
iv-mobile	Recapito telefonico cellulare
iv-tel	Recapito telefonico
iv-fax	Numero di fax
iv-mailp	Indirizzo e-mail personale dell'utente interno (solo utenti interni)
iv-ou1	Macro-struttura in cui è inserito l'utente interno nell'organizzazione di Roma Capitale (solo utenti interni)
iv-ou2	Organizzazione di secondo livello in cui è inserito l'utente (solo utenti interni)
iv-ou3	Organizzazione di terzo livello in cui è inserito l'utente (solo utenti interni)
iv-matr	Numero individuale identificativo dell'utente (solo utenti interni)
iv-rapp	Tipologia di rapporto di lavoro per l'utente (solo utenti interni)
iv-liv	Livello di inquadramento dell'utente (solo utenti interni)
iv-prof	Professione (solo per utenti esterni)

Tabella 2: Variabili fornite nell'header HTTP dal servizio IAM

In particolare la variabile **iv-user** contiene l'identificativo univoco dell'utente, generalmente rappresentato dal codice fiscale per gli utenti esterni (es.: i cittadini registrati per l'uso dei servizi on-line offerti dal portale di Roma Capitale), una stringa formata dalla composizione del nome proprio e del cognome, separati da un punto per gli utenti interni (es.: "mario.rossi" per il sig. Mario Rossi, oppure "mariapia.digiovanni" per la sig.ra Maria Pia Di Giovanni).

Il codice fiscale dell'utente viene garantito nella variabile **iv-codfis**.

Per venire incontro a specifiche esigenze applicative è possibile comporre i valori di due o più variabili della Tabella 2, raccogliendo quei valori in una sola variabile. Ad esempio è possibile definire una variabile come **iv-indirizzo** raccogliendo tutti i dati di un indirizzo di domicilio o di residenza (es.: via, numero civico, CAP, comune e provincia).

La variabile **iv-portal-groups** contiene l'elenco dei gruppi LDAP a cui appartiene l'utente; l'appartenenza a tali gruppi può essere utilizzata come elemento per stabilire macroscopicamente se l'utente è abilitato o meno ad usufruire di una determinata funzione o ad accedere ad una determinata applicazione.

La stringa presente nella variabile **iv-portal-groups** ha il seguente formato:

```
cn=gruppo1\,ou=Groups\,dc=cdr\,dc=it,cn=gruppo2\,ou=Groups\,dc=cdr\,dc=it,...,  
cn=gruppon\,ou=Groups\,dc=cdr\,dc=it
```

I nomi identificativi dei gruppi sono riportati con un *path* LDAP completo; i *path* di ciascun gruppo è separato dal gruppo successivo mediante il carattere ",", (virgola); le componenti del *path* LDAP sono separate dalla sequenza "\", (backslash virgola); il nome della componente del *path* LDAP è separata dal valore con il carattere "=" (uguale).

3.3 Informazioni sulla persona giuridica rappresentata dalla persona fisica o delegata

Qualora, a valle dell'autenticazione come "persona fisica", l'utente intenda operare come rappresentante di una persona giuridica per conto della quale possiede dei titoli di rappresentanza (registrati su Registro Imprese di Infocamere, su altra sorgente informativa autoritativa e integrata con la componente "Traduttore-PG" oppure attraverso conferimento di specifiche deleghe), tra le variabili header inserite nella request HTTP da Access Manager, potranno essere inserite anche quelle riportate in **Tabella 3**.

Variabile	Descrizione
IV-PG-CODFIS	Codice Fiscale della persona giuridica per la quale intende operare
IV-PG-PIVA	Partita IVA della persona giuridica
IV-PG-NATURA	Natura Giuridica della persona giuridica (SRL, SPA, ecc.)
IV-PG-RAG-SOC	Ragione sociale (Denominazione) del Soggetto PG/UL
IV-PG-INDIRIZZO	Denominazione (toponimo) dell'Indirizzo
IV-PG-COM-IND	Denominazione del Comune dell'Indirizzo
IV-PG-PROV-IND	Sigla della provincia del Comune dell'Indirizzo
IV-PG-CAP-IND	CAP dell'indirizzo
IV-PG-CIV-IND	Numero civico dell'Indirizzo
IV-PG-ESP-IND	Esponente del civico dell'indirizzo
IV-PG-RUOLO	Carica o ruolo della PF relativamente alla persona giuridica

Variabile	Descrizione
IV-PG-DELEGA	Indica se l'utente sul soggetto PG per cui si vuole operare è stato abilitato mediante delega. Valori ammessi: S – Se abilitato mediante delega N – Se non è abilitato mediante delega
IV-PG-DT-FINE-VAL-DELEGA	Indica la data di validità della delega conferita sul soggetto PG all'utente. Formato dd/MM/yyyy hh:mm
IV-PG-CCIAA	Codice di iscrizione Camera del Commercio, Industria, Artigianato e Agricoltura
IV-PG-NREA	Identificativo iscrizione Repertorio Economico Amministrativo.
IV-COD-CAT-GIURDICA	È la categoria giuridica di appartenenza del soggetto PG selezionato. Ad esempio, se si seleziona un soggetto nell'elenco delle Imprese, assumerà il valore RAPPRESENTANTE_IMPRESA.
IV-CONSENSO-GDPR	Indica se l'utente sul soggetto PG per cui vuole operare ha il consenso GDPR. Valori ammessi: S – Se ha il consenso GDPR N – Se non ha il consenso GDPR

Tabella 3: Variabili fornite nell'header HTTP dal servizio IAM per rappresentanti di persone giuridiche

Le informazioni riportate in tabella si aggiungono a quelle relative alla persona fisica; pertanto, l'intenzione dell'utente di operare come rappresentante di una persona giuridica, può essere rilevata dall'applicazione che riceve request HTTP con tali variabili, attraverso la verifica della presenza dell'attributo IV-PG-PIVA e IV-PG-CODFIS che rappresentano rispettivamente la Partita IVA e il Codice Fiscale della persona giuridica rappresentata dall'utente.

3.4 Autenticazione con SPID

Il Portale Istituzionale di Roma Capitale e il sistema di controllo degli accessi ai servizi on-line destinati ai cittadini e alle aree riservate del portale stesso, garantiscono l'accesso degli utenti in possesso di un'identità digitale SPID (Sistema Pubblico di Identificazione Digitale¹), ottenuta da un Identity Provider accreditato presso AgID. In questo caso il processo di accreditamento e la gestione dei dati identificativi dell'utente non sono di pertinenza del sistema IAM di Roma Capitale, ma attengono alle competenze dei sistemi on-line del Identity Provider.

Per la gestione delle utenze autenticate con SPID, il sistema IAM garantisce però alle applicazioni on-line integrate con il Portale, un'interfaccia applicativa omogenea analoga a quella già utilizzata per gli utenti autenticati dal Portale stesso.

L'interfaccia viene garantita attraverso l'uso delle *HTTP header variable*, fornite dal sistema Access Manager alle applicazioni.

¹ Si veda, ad esempio: <http://www.spid.gov.it>

3.5 Codifica dei caratteri

In linea con quanto previsto dalle RFC 2822² e RFC 5322³, il testo dell'header HTTP deve essere rappresentato con caratteri ASCII standard (codici ASCII da 0 a 127). Di conseguenza anche il valore delle variabili inserite nell'header HTTP dal sistema IAM devono rispettare tale codifica. Tuttavia, può capitare che i valori delle variabili header contengano invece caratteri che non trovano una corrispondenza nei codici ASCII standard (da 0 a 127): è il caso delle lettere accentate molto comuni nella lingua italiana o di altri simboli particolari utilizzati in alcune lingue straniere (es.: i caratteri "ç" e "ñ" utilizzati nella lingua spagnola o i caratteri "ß" e "ü" utilizzati nel tedesco). In questi casi il valore delle variabili deve essere codificato in modo da ricondurlo ad una stringa di caratteri ASCII standard.

Secondo quanto riportato nella RFC 2047⁴ le stringhe contenenti caratteri ASCII non standard vengono codificate con una stringa che inizia con la sequenza "=?", termina con "?=" e contiene al suo interno due caratteri "?"; i quattro punti interrogativi delimitano le seguenti componenti:

- **charset**: è uno dei character set registrati presso IANA per l'uso della codifica secondo lo standard MIME;
- **encoding**: è un singolo carattere; può essere "B" o "Q", dove "B" significa che la codifica è in Base 64, mentre "Q" indica una codifica definita nella RFC 2045.
- **encoded-text**: è la stringa codificata in accordo a quanto specificato in *encoding*.

=?charset?encoding?encoded-text?=?

Nella codifica dei valori delle HTTP header variables contenenti caratteri non standard effettuata dal sistema IAM di Roma Capitale, viene utilizzato il character set UTF-8 e la codifica Base 64. Una tipica stringa codificata dal sistema IAM assume pertanto la seguente forma:

=?UTF-8?B?encoded-text?=?

Nell'uso delle HTTP header variable da parte delle applicazioni è necessario, pertanto, verificare se il valore rispetta la codifica sopra descritta e, in tal caso, decodificare la stringa per poi poterla utilizzare "in chiaro". Riportiamo di seguito due esempi in linguaggio Java e in C# in ambiente Microsoft.Net.

3.5.1 JEE con Java 6 e 7

Supponiamo che "inputString" sia il valore della stringa acquisita da una HTTP header variable; questo frammento di codice restituisce la stringa in formato "leggibile".

```
import javax.xml.bind.DataConverter;
import java.nio.charset.Charset;

String encodedString = inputString.split("=\\?UTF-8\\?B\\?")[1].split("\\?=")[0];
byte[] decoded = DataConverter.parseBase64Binary(encodedString);
Charset c = Charset.forName("utf-8");
String readableString = new String(decoded, c);
return readableString;
```

² Si veda <https://tools.ietf.org/html/rfc2822>

³ Si veda <https://tools.ietf.org/html/rfc5322>

⁴ Si veda <https://tools.ietf.org/html/rfc2047>

3.5.2 JEE con Java 8

Con la versione 8 di JDK si può utilizzare il package Base64; anche in questo caso supponiamo che “inputString” sia il valore della stringa acquisita da una HTTP header variable; il seguente frammento di codice restituisce la stringa in formato “leggibile”.

```
import java.nio.charset.Charset;
import java.util.Base64;

String encodedString = inputString.split("\\?UTF-8\\?B\\?") [1].split("\\?=") [0];
byte[] decoded = Base64.getDecoder().decode(encodedString);
Charset c = Charset.forName("utf-8");
String readableString = new String(decoded, c);
return readableString;
```

3.5.3 Microsoft .net – C#

Anche in quest’ultimo caso supponiamo che “inputString” sia il valore della stringa acquisita da una HTTP header variable; il seguente frammento di codice restituisce la stringa in formato “leggibile”.

```
String encodedString = inputString.Split(new string[] { "\\?UTF-8\\?B\\?" },
StringSplitOptions.None)[1].Split(new string[] { "\\?=" },
StringSplitOptions.None)[0];
var base64EncodedBytes = System.Convert.FromBase64String(encodedString);
return System.Text.Encoding.UTF8.GetString(base64EncodedBytes);
```

3.6 Autenticazione con OIDC

Il sistema di Access Management di Roma Capitale supporta il protocollo di integrazione OpenID Connect (OIDC), come specificato nel Paragrafo 2.4. Si raccomanda di adottare questa modalità di integrazione per le applicazioni progettate secondo il paradigma delle “single page application”.

3.7 Claim e scope supportati

Nell’autenticazione OIDC, il **claim** sta ad indicare una singola proprietà del soggetto autenticato. Nel caso dell’integrazione col sistema IAM di Roma Capitale, ogni claim fa riferimento ad uno specifico attributo dell’utente, tra quelli descritti in Tabella 2 a pagina 13. Inoltre, come da specifica, sarà sempre presente nell’id_token o nelle risposte dell’endpoint userinfo, il claim “sub” (Subject) che conterrà lo username dell’utente: codice fiscale per i cittadini e una stringa del tipo “nome.cognome” per i dipendenti.

Gli **scope**, invece, sono raggruppamenti logici dei claim. Attualmente, il sistema IAM implementa come da specifica lo scope “**profile**”, che contiene i seguenti claim: iv_user, iv_nome, iv_cognome, iv_codfis, iv_email.

Infine, per far fronte a delle specifiche richieste implementative, è stato definito un ulteriore scope, denominato “**tipo_utente**”, che contiene l’attributo “iv_tipoutente”. Tale attributo sarà valorizzato come “cittadino” qualora l’utente autenticato effettivamente un cittadino, o, viceversa, sarà valorizzato come “dipendente”.

3.7.1 Specifiche tecniche per l'integrazione

L'integrazione delle applicazioni, utilizzando il protocollo OIDC, viene realizzata in due passaggi: la pubblicazione dell'applicazione on-line sul Portale istituzionale attraverso il sistema di reverse proxy di Portale, e l'effettiva integrazione coi sistemi di autenticazione.

In particolare, l'integrazione con il sistema IAM, si compone dei seguenti punti:

1. creazione di una coppia di credenziali (**client_id** e **client_password**) da condividere per via sicura con i referenti dell'applicazione;
2. condivisione col team di gestione del sistema IAM delle **redirection URI** applicative;
3. concordare coi referenti applicativi gli **scope** che potranno essere richiesti da parte del servizio autenticato;
4. condivisione con i referenti applicativi degli endpoint di **authorization**, **userinfo** e **token**.

3.7.2 Il processo di autenticazione e richiesta degli attributi utente

Riportiamo, per comodità di lettura, lo stesso diagramma di sequenza già presentato a 9, con la descrizione degli step del processo di autenticazione basato sul protocollo OIDC.

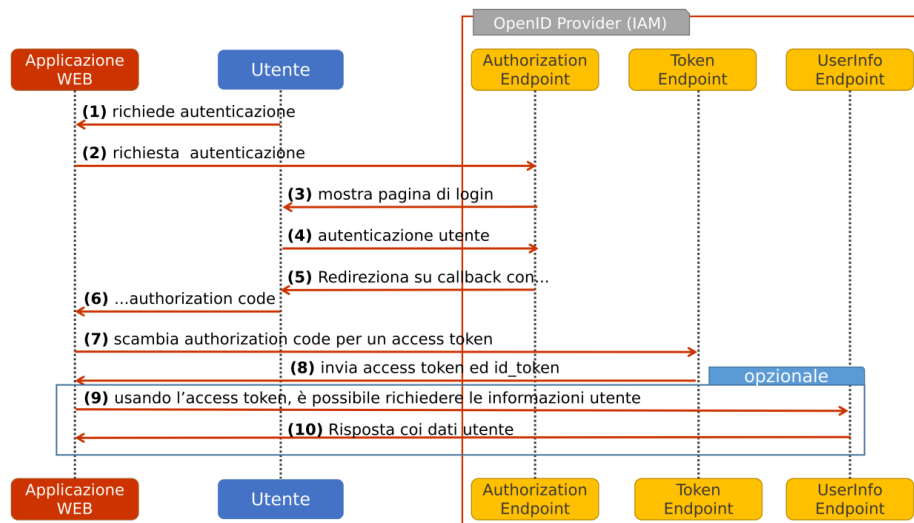


Figura 7: Sequence diagram della autenticazione di un utente con protocollo OIDC

Nel momento in cui l'utente sceglie di autenticarsi sulla web application (1), l'evento, deve scatenare la richiesta di autorizzazione verso l'authorization endpoint del sistema IAM (2), indicando contestualmente nella *queryString* i parametri **client_id**, **redirect_uri**, **scope**, **response_type=code**, **response_mode** e **nonce** (valore random per evitare attacchi di tipo *replay attack*).

Di seguito riportiamo un esempio di questo tipo di chiamata sotto forma di request HTTP GET verso l'ambiente di pre-produzione del sistema IAM (ssopre.comune.roma.it):

```
https://ssopre.comune.roma.it/ssoservice/oauth2/realms/root/realms/public/authorize?client_id=oidcClient&redirect_uri=https://preprod.comune.roma.it/oidcClient/callback&scope=openid&tipo_utente&response_type=code&response_mode=form_post&nonce=off41zewan9
```

Se l'utente non risulta già autenticato, il front-end di access management si occupa di presentare la form di autenticazione (3) (che prevede la possibilità di autenticarsi con credenziali SPID, CIE, CNS, mentre per i dipendenti il meccanismo è di tipo username e password).

A valle di un'autenticazione avvenuta con successo (4), il sistema IAM risponderà sulla *redirect_uri* (5) e (6), utilizzando la *response_type* specificata precedentemente, indicando gli attributi **iss** (identificativo

dell'issuer), **scope**, **client_id** e **code**; quest'ultimo è l'**authorization code** con cui richiedere all'endpoint token i token di accesso e di refresh.

Una possibile risposta dell'access manager è riassunta nella seguente HTTP GET. Gli attributi possono essere anche inviati alla callback url con metodo HTTP POST.

```
https://preprod.comune.roma.it/oidcClient/callback?
code=2c9ffc2a-7e05-4ea5-a925-03cf7c53e897&scope=openid&tipo_utente&
iss=https://ssopre.comune.roma.it:443/ssoservice/oauth2/realms/root/realms/
public&client_id=oidcClient
```

Successivamente alla ricezione dell'autorization code, quindi, per scambiare il suddetto codice per i token, sarà necessario eseguire una richiesta HTTP POST all'endpoint **access_token** (7). Come esempio, utilizziamo lo strumento "curl" come riportato di seguito:

```
curl --location --request POST
'https://ssopre.comune.roma.it/ssoservice/oauth2/realms/root/realms/public/
access_token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=oidcClient' \
--data-urlencode 'client_secret=oidcClientP4sswd.123' \
--data-urlencode 'grant_type=authorization_code' \
--data-urlencode 'redirect_uri=https://preprod.comune.roma.it/oidcClient/callback' \
--data-urlencode 'code=2c9ffc2a-7e05-4ea5-a925-03cf7c53e897'
```

Nell'esempio i parametri **client_id** e **client_secret** sono le credenziali condivise al **punto 1** delle specifiche tecniche, mentre **grant_type=authorization_code** è usata per indicare la volontà di scambiare un *authentication code* (ottenuto attraverso la GET precedente) con un access token.

L'access manager, risponderà come nel passo (8) del diagramma riportato in figura con una response di questo tipo:

```
{
  "access_token": "eyJ0eXAiOiJKV1Qi...G7p6_1YkRXg",
  "refresh_token": "eyJ0eXAiOiJKV1Qi...Ksef-CTXv10A",
  "scope": "openid tipo_utente",
  "id_token": "eyJ0eXAiOiJK...M4Olo6IdL0k",
  "token_type": "Bearer",
  "expires_in": 3599,
  "nonce": "ymq2pgimusd"
}
```

Il parametro **id_token** è codificato in Base64 e può essere decodificato per ottenere le informazioni utente, come in questo caso (notare la presenza degli attributi "sub" e "iv_tipoutente"):

```
{ "typ": "JWT", "alg": "HS256" }
{ "at_hash": "p2LBjFxFxXaZCqDsem39lW1w",
  "sub": "BNCMRC92M30G148K",
  "auditTrackingId": "ee05dc9d-9ec1-4679-a660-dc0ddc8663b8-20210",
  "iss": "https://ssopre.comune.roma.it:443/ssoservice/oauth2/realms/root/realms/
public",
  "tokenName": "id_token",
  "nonce": "ymq2pgimusd",
  "aud": "oidcClient",
  "c_hash": "TgSn9rJN1hDB0Nlp7bs-Yw",
  "org.forgerock.openidconnect.ops": "a0200085-763a-472f-ba41-88015f3721b4",
  "auth.time": 1647980540,
  "azp": "oidcClient",
  "iv_tipoutente": "cittadino",
  "realm": "/public", "exp": 1647985734,
  "tokenType": "JWTToken",
  "iat": 1647982134 }
```

Infine, sarà eventualmente possibile ricevere di nuovo gli attributi utente, ssecondo gli scope specificati negli scopes condivisi, scambiando l'access token finché risulta valido **(9)**. Di seguito una chiamata del comando "curl" come esempio:

```
curl --location --request POST
'https://ssopre.comune.roma.it/ssoservice/oauth2/realms/root/realms/public/userinfo' \
--header 'Authorization: Bearer eyJ0eXAiOiJKV1Qi...G7p6_1YkRXg'
```

La risposta conseguente a tale chiamata da parte dell'Access Manager (passo **(10)** del sequence diagram) è la seguente:

```
{
  "sub": "BNCMRC92M30G148K",
  "iv_tipoutente": "cittadino"
}
```

4 Processo di configurazione degli ambienti di esercizio e pre-esercizio

Sul sistema informativo di Roma Capitale sono definiti due ambienti distinti, uno di **pre-produzione**, dedicato al test e al collaudo delle applicazioni, ed uno di **produzione**, dedicato all'esercizio delle applicazioni. Gli ambienti, come descritto nelle pagine precedenti, sono costituiti da diverse componenti integrate fra loro, gestite da team distinti: pertanto è opportuno attenersi a quanto descritto di seguito per garantire la corretta configurazione e documentazione della configurazione dell'infrastruttura.

Le operazioni di configurazione sono differenti per applicazioni Internet (accessibili dai cittadini o dai dipendenti di Roma Capitale attraverso il Portale Istituzionale e la rete Internet), o intranet (applicazioni riservate ai dipendenti, accessibili solo attraverso la rete interna di Roma Capitale), ma anche per applicazioni pubbliche, ad accesso anonimo, che non richiedono operazioni di autenticazione o per applicazioni riservate, che richiedono l'autenticazione e l'autorizzazione degli utenti. In è riportato uno schema che riassume le possibili configurazioni applicative.

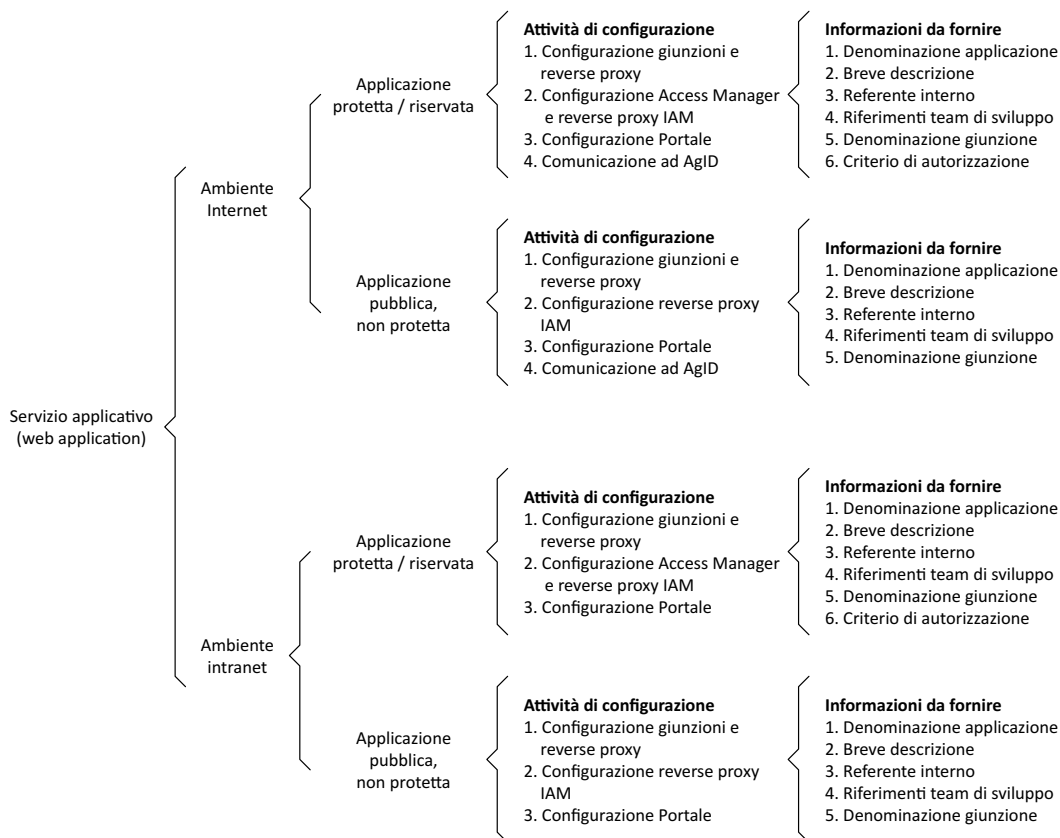


Figura 8: Schematizzazione delle possibili configurazioni applicative

4.1 Informazioni necessarie per la configurazione degli ambienti Portale e IAM

Al fine di garantire la corretta e tempestiva configurazione degli ambienti di pre-produzione e di produzione e il mantenimento delle informazioni necessarie alla corretta gestione della configurazione applicativa, è

necessario, a valle della configurazione dell'ambiente application server e delle infrastrutture centrali di sicurezza gestite da RTI Sistemi Centrali, trasmettere le seguenti informazioni al Presidio Sistema IAM, che provvederà a condividere quanto di competenza, anche con il Presidio Portale Istituzionale.

- **Denominazione dell'applicazione o del servizio**
Nome dell'applicazione da riportare sui link del Portale o di altre pagine che ne contengano i riferimenti.
- **Contesto di business**
Area di business in cui si inserisce il servizio erogato dall'applicazione (es.: Servizi tributari, Servizi scolastici, ecc.).
- **Breve descrizione dell'applicazione o del servizio**
Descrizione del servizio erogato dall'applicazione, in modo tale da guidare l'utente nella scelta dei servizi da selezionare; la descrizione deve essere comprensibile anche per quanti non hanno dimestichezza con il "gergo" adottato nell'ambito dei servizi applicativi di Roma Capitale.
- **Nominativo e riferimenti del referente interno**
Nominativo, numero di telefono e indirizzo e-mail del funzionario di Roma Capitale che svolge il ruolo di referente per il servizio applicativo.
- **Azienda a cui è affidato lo sviluppo o la manutenzione dell'applicazione**
Denominazione del fornitore che ha in carico l'attività di sviluppo software, di manutenzione o di gestione tecnica del servizio applicativo.
- **Nominativo e riferimenti del referente aziendale**
Nominativo, numero telefonico e indirizzo e-mail di un referente tecnico del fornitore.
- **Giunzione dell'applicazione**
Path con cui è stata definita la giunzione sugli apparati di sicurezza dei Sistemi Centrali (es.: reverse proxy). Questa informazione deve essere concordata con il gruppo RTI Sistemi (e-mail: rti.salamacchine@comune.roma.it).
- **Criterio di autorizzazione degli utenti**
Denominazione dei gruppi o dei profili autorizzativi che devono essere definiti sul sistema di controllo accessi (Access Manager) per regolare le autorizzazioni di accesso all'applicazione (es.: accesso libero/anonimo, accesso riservato agli utenti esterni, accesso riservato ai dipendenti interni, ecc.).
- **Ambito IT dell'applicazione**
Ambito IT in cui viene rilasciata l'applicazione, distinguendo tra applicazione Internet accessibile sul portale Istituzionale, applicazione intranet accessibile solo dalla rete di Roma Capitale.
- **Utenze da abilitare sull'ambiente di pre-produzione**
Elenco delle utenze da abilitare sull'ambiente di pre-produzione (con il relativo ruolo) per l'esecuzione di test, verifiche di integrazione e operazioni di collaudo. Le utenze sono nominative, rilasciate ai referenti interni o esterni dell'applicazione. Qualora il fornitore sia lo stesso, si suggerisce di riutilizzare le stesse utenze anche per applicazioni differenti.

La comunicazione delle informazioni sopra elencate dovrà essere effettuata via e-mail, indirizzandola al gruppo di **Presidio Sistema IAM** (presidiosupportoutentiesterni@comune.roma.it) e per conoscenza al **referente del Servizio Internet** (servizio.internet@comune.roma.it) e al **Referente Applicativo Interno**, compilando il modulo riportato nella pagina seguente, in ogni sua parte.


4.2 Riferimenti dei gruppi di gestione

Di seguito sono riportati gli indirizzi e-mail con cui è possibile contattare i team che si occupano del processo di configurazione e gestione delle infrastrutture di pre-produzione e di produzione.

Denominazione	E-mail	Compiti
Servizio Internet	servizio.internet@comune.roma.it	Coordina le attività dei gruppi di supporto sistemistico; è l'interfaccia principale con i referenti interni dei servizi applicativi
RTI Sistemi Centrali	rti.salamacchine@comune.roma.it	Gestisce la configurazione dell'infrastruttura di sicurezza e di reverse proxy posta di fronte ai server applicativi
Presidio Sistema IAM	presidiosupportoutentiesterni@comune.roma.it	Gestisce la configurazione del sistema Identity and Access Management
Presidio Portale Istituzionale	presidiosupportoportale@comune.roma.it	Gestisce la configurazione del Portale Istituzionale

Tabella 4: Riferimenti dei gruppi coinvolti nel processo di gestione delle infrastrutture applicative

Roma Capitale
Dipartimento Innovazione Tecnologica
Scheda di definizione del servizio applicativo

ROMA 	
Dipartimento Innovazione Tecnologica	
Applicazione	Denominazione
	Contesto di business
	Altri ambiti
	Descrizione del servizio
	URL
	Giunzione
	Altra giunzione
	Ambito IT
	Configurazione tecnica
	Configurazione tecnica (altro)
	Criterio di autorizzazione
	Altro criterio di autorizzazione
	Utenze da abilitare in ambiente di pre-produzione
	Nome
Cognome	
CF	
E-mail	
Tipo	
Ruolo	
Referente interno	Nominativo
	Dipartimento / Ufficio
	Telefono fisso
	Telefono cellulare
	E-mail
Referente esterno	Azienda / RTI
	Nominativo
	Telefono fisso
	Telefono cellulare
	E-mail