Smart Cities and Communities and Social Innovation
Bando MIUR
D.D. 391/Ric. del 5 luglio 2012

Framework di sicurezza della piattaforma OCP (Identity & Access Management)

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

AAI: Il problema che OCP ha affrontato

- Le PA hanno come riferimento dei Data Center eterogenei che usano sistemi di identificazione, autorizzazione e controllo degli accessi ai servizi diversi

- L'accesso a servizi offerti dalle PA in domini amministrativi diversi e ancora di più la collaborazione tra servizi di domini amministrativi diversi può avvenire solo per mezzo di un framework di sicurezza AAI comune e condiviso

- Anche se SPID ha finalmente reso disponibile un'unica tecnologia per l'autenticazione a livello nazionale, gestire utenti e privilegi per Data Center e servizi distribuiti in modo dinamico e sicuro è molto complesso

- Anche il semplice accesso da parte di un utente generico SPID ai servizi offerti da PA diverse oggi è problematico

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

La soluzione: il framework di sicurezza di OCP

Architettura Service Oriented, risultato di uno sviluppo guidato da 4 principi fondamentali:

- Autenticazione Federata (SPID)
- Autorizzazione (XACML3)
- Interoperabilità (Policy Decision as a Service, Policy Administration as a Service)
- Delega di credenziali (OAuth2)

Soddisfa le esigenze di sicurezza degli scenari seguenti, con diversi domini di autenticazione:

- Scenario Locale
  Il servizio erogato dalla PA, la risorsa protetta & l'utente sono gestiti nello stesso dominio
- Scenario Federazione di Access Manager
  Il servizio erogato dalla PA & la risorsa protetta sono in un dominio MA l'utente è gestito in altro dominio
- Scenario Federato & Geograficamente distribuito
  Il servizio erogato dalla PA, la risorsa protetta & l'utente sono gestiti in domini geograficamente distribuiti

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Delega di credenziali & composizione di servizi

La delega di credenziali è un requisito trasversale a **tutti** gli scenari supportati dal framework di sicurezza di OCP

Il requisito che deve soddisfare è quello di una richiesta che per essere eseguita necessita a sua volta una composizione di servizi che devono operare a nome del richiedente iniziale

- Servizi in cascata che agiscono a nome dello stesso utente

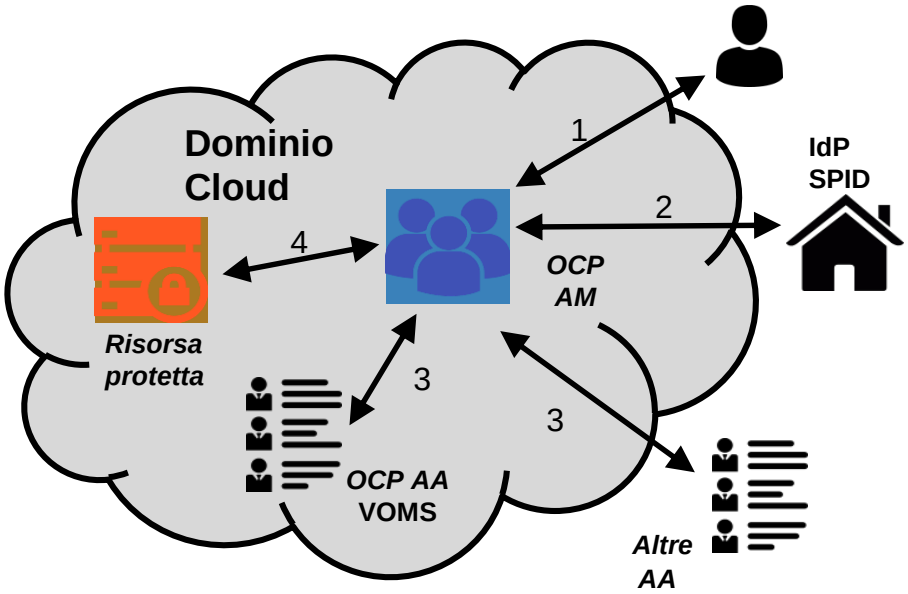
Lo sviluppo della delega di credenziali sta avvenendo in collaborazione con il progetto europeo INDIGO-Datacloud ed ha come tecnologia di riferimento OAuth2

- Sono al vaglio diversi modelli: Cross client tokens, Macaroons, OAuth token exchange

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Scenario locale

Il servizio erogato dalla PA, la risorsa protetta & l'utente sono gestiti nello stesso dominio

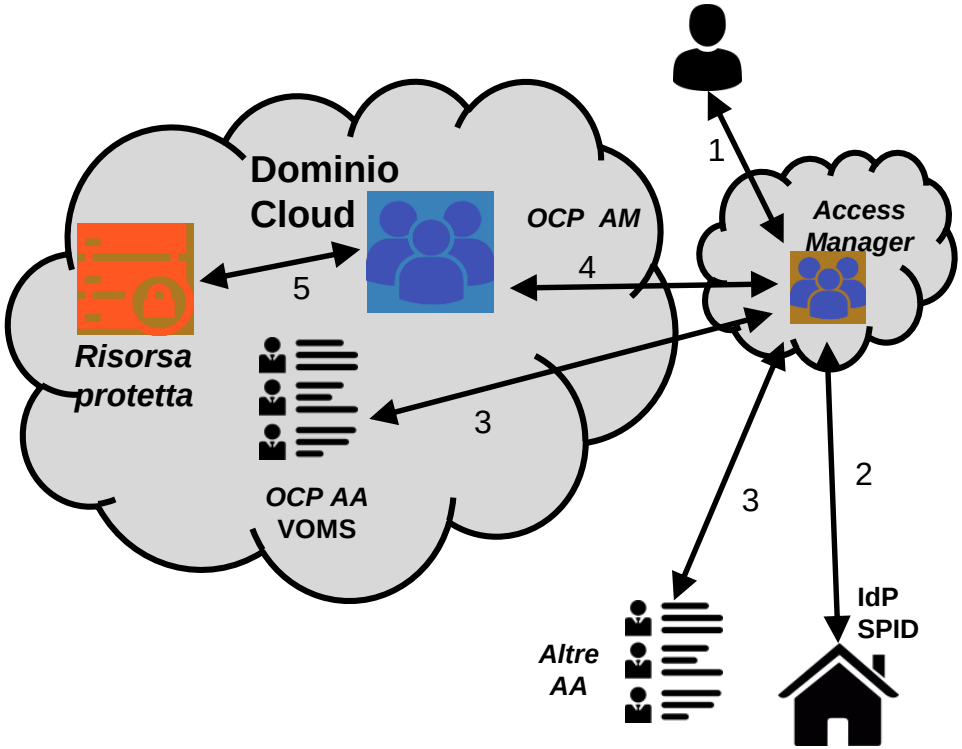


1. L'utente chiede l'accesso alla risorsa protetta tramite browser
2. La richiesta viene intercettata da OCP Access Manager che avvia il processo di verifica dell'identità attivando i servizi di accesso all'Identity Provider SPID indicato dall'utente
3. OCP Access Manager arricchisce l'asserzione di identità interrogando l'attribute authority di OCP o di terze parti
4. OCP Access Manager verifica sulla base dell'asserzione e degli attributi, il profilo autorizzativo dell'utente ed effettua l'enforcement verso la risorsa protetta

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Scenario federazione di Access Manager

Il servizio erogato dalla PA & la risorsa protetta sono in un dominio MA l'utente è gestito in altro dominio

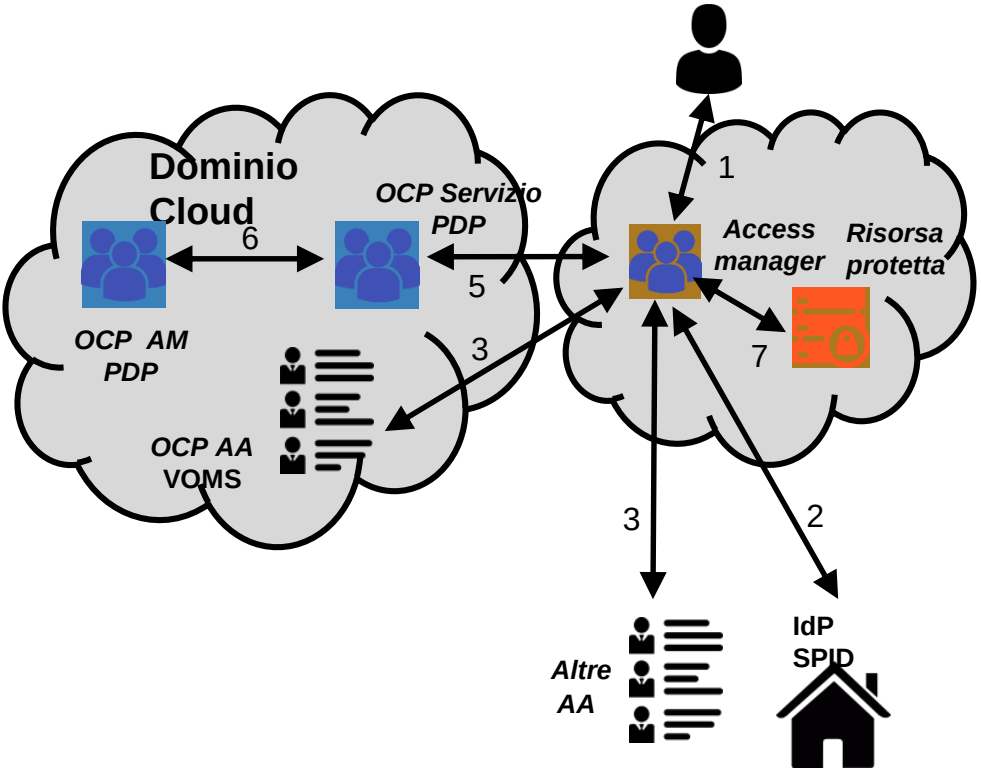


1. L'utente chiede l'accesso alla risorsa protetta tramite il browser
2. La richiesta viene intercettata da un access manager facente parte di un altro dominio; l'access manager avvia il processo di verifica della identità accedendo all'IdP SPID indicato dall'utente
3. l'access manager arricchisce l'asserzione di identità interrogando l'attribute authority di OCP o di terze parti
4. l'access manager trasferisce l'identità dell'utente e relativi attributi all'OCP Access Manager (es. costruisce un'asserzione SAML)
5. OCP Access Manager applica l'enforcement verso la risorsa protetta

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Scenario federato e geograficamente distribuito

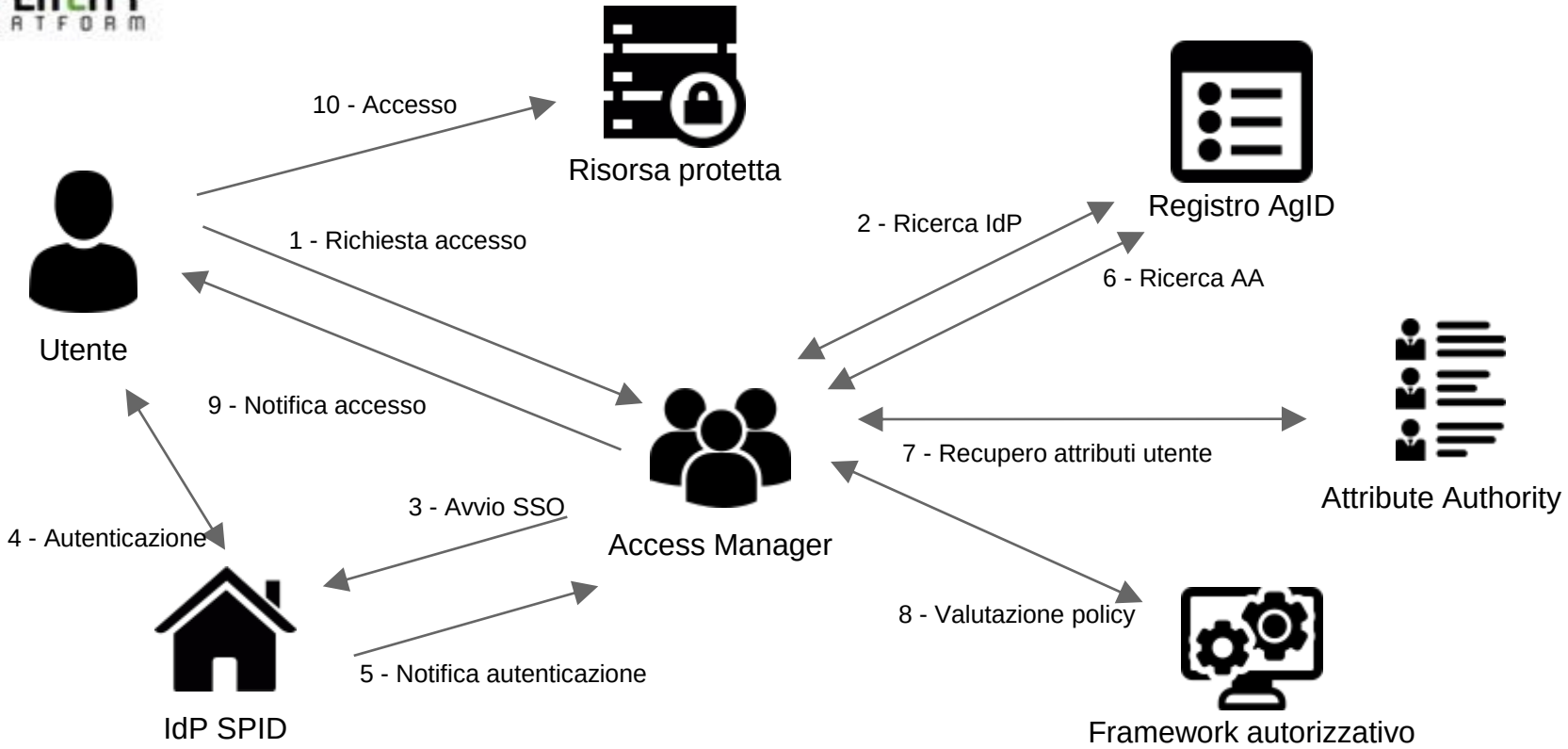
Il servizio erogato dalla PA, la risorsa protetta & l'utente sono gestiti in domini geograficamente distribuiti



1. L'utente chiede l'accesso alla risorsa protetta tramite il browser
2. La richiesta viene intercettata da un access manager facente parte di un altro dominio; access manager avvia il processo di verifica dell'identità accedendo all'Identity Provider SPID indicato dall'utente
3. access manager arricchisce l'asserzione di identità interrogando l'attribute authority di OCP o di terze parti
4. access manager costruisce un'asserzione di autenticazione arricchita degli attributi dell'utente e la invia al servizio OCP PDP (es asserzione SAML)
5. Il servizio OCP PDP consuma l'asserzione, richiede una policy decision al PDP OCP Access Manager e riceve da questi una policy response
6. Il servizio OCP PDP trasmette all'access manager la policy response
7. l'access manager applica l'enforcement verso la risorsa protetta in base alla policy response ottenuta

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Autenticazione via SPID



Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

Tecnologie utilizzate (I)

Attribute Authority:

- Compatibile con quanto riportato nella sezione **“Regole tecniche per il gestore di attributi qualificati”** della specifica SPID
- Accesso via **TLS 1.2,** autorizzazione modulare: implementazione proposta basata su standard XACML
- Gestione di utenti, gruppi ed attributi via web API (standard SCIM 1.1)

Framework autorizzativo:

- i Servizi PDP e PAP sono basati sullo standard **“eXtensible Access Control Markup Language v.3.0”** di OpenAM
- I servizi PDP e PAP sono esterni all’Access Manager OpenAM ma utilizzano le API messe a disposizione da OpenAM
- i servizi PDP e PAP forniscono una interfaccia standard, verificano l’asserzione di autenticazione (attualmente SAML) e le caratteristiche della richiesta, trasformano la richiesta nel formato previsto da OpenAM (proprietario) e la inviano/ricevono con le modalità previste da OpenAM.

Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca

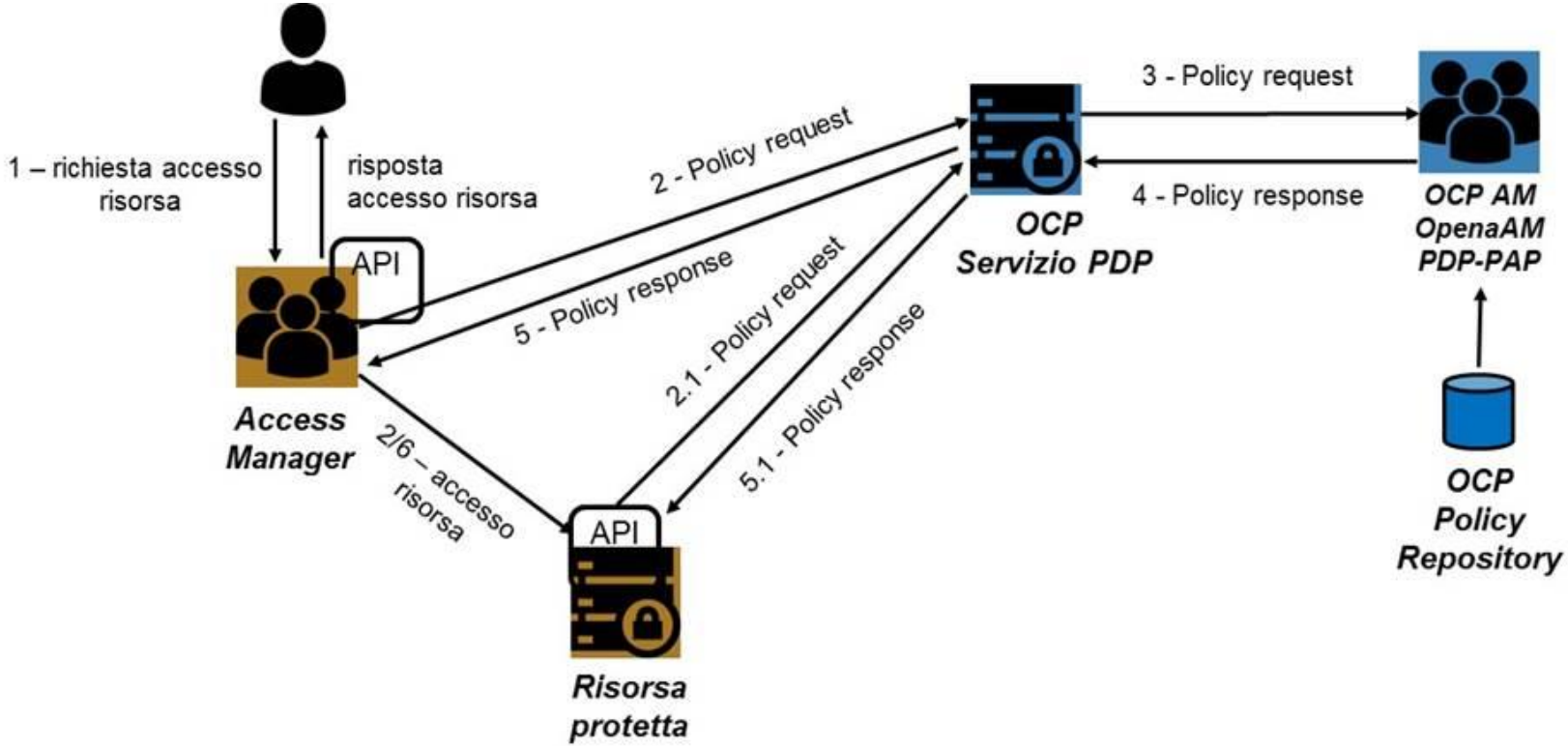
Tecnologie utilizzate (II)

Access Manager:

- L’ Access Manager di OCP per le web application è basata su OpenAM ed OpenIG
- OpenAM agisce da centro di riferimento per:
  - Gestione del SSO via SPID
  - Aggregazione di attributi
  - Gestione dell’autorizzazione
- OpenIG è la barriera d’ingresso (reverse proxy) che protegge la web application
- L’implementazione ha impatto minimo sullo sviluppo di una web application ed è completamente indipendente dal linguaggio e dalla tecnologia usata

Open City Platform è un progetto finanziato da Ministero dell’Istruzione, dell’Università e della Ricerca

Servizio di Policy Decision



Open City Platform è un progetto finanziato da Ministero dell'Istruzione, dell'Università e della Ricerca