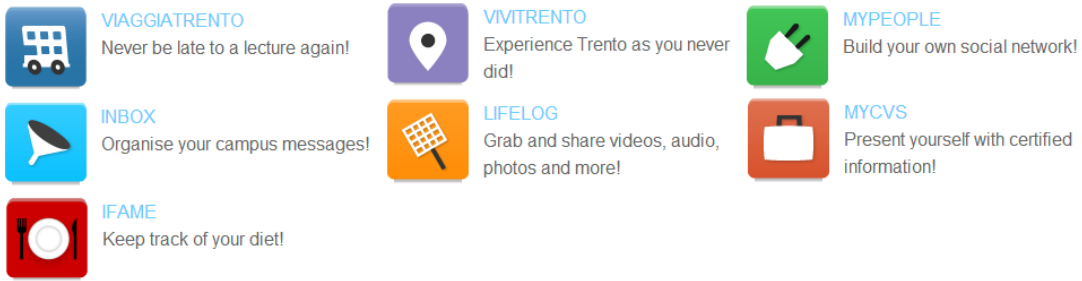
Smart Campus Project: API Manager

Giada Sciarretta - October 21, 2014

Outline

- Smart Campus Overview
- API Manager Overview
- User Policies
- CPR tool Extension and Automated Test Case Generation

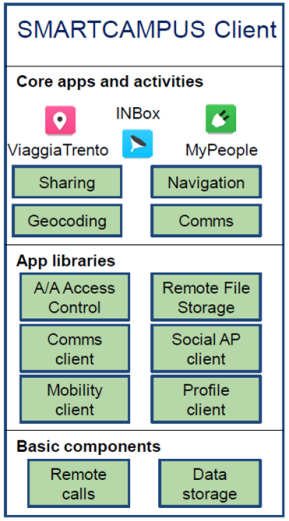
SmartCampus is a TrentoRise project that provides a growing set of services to help students and citizens manage their everyday life in Trento.

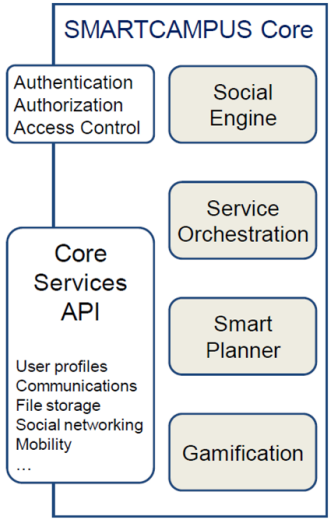


What is SmartCampus Project?

- Control the access to the user data in the platform
- Differentiate between different apps

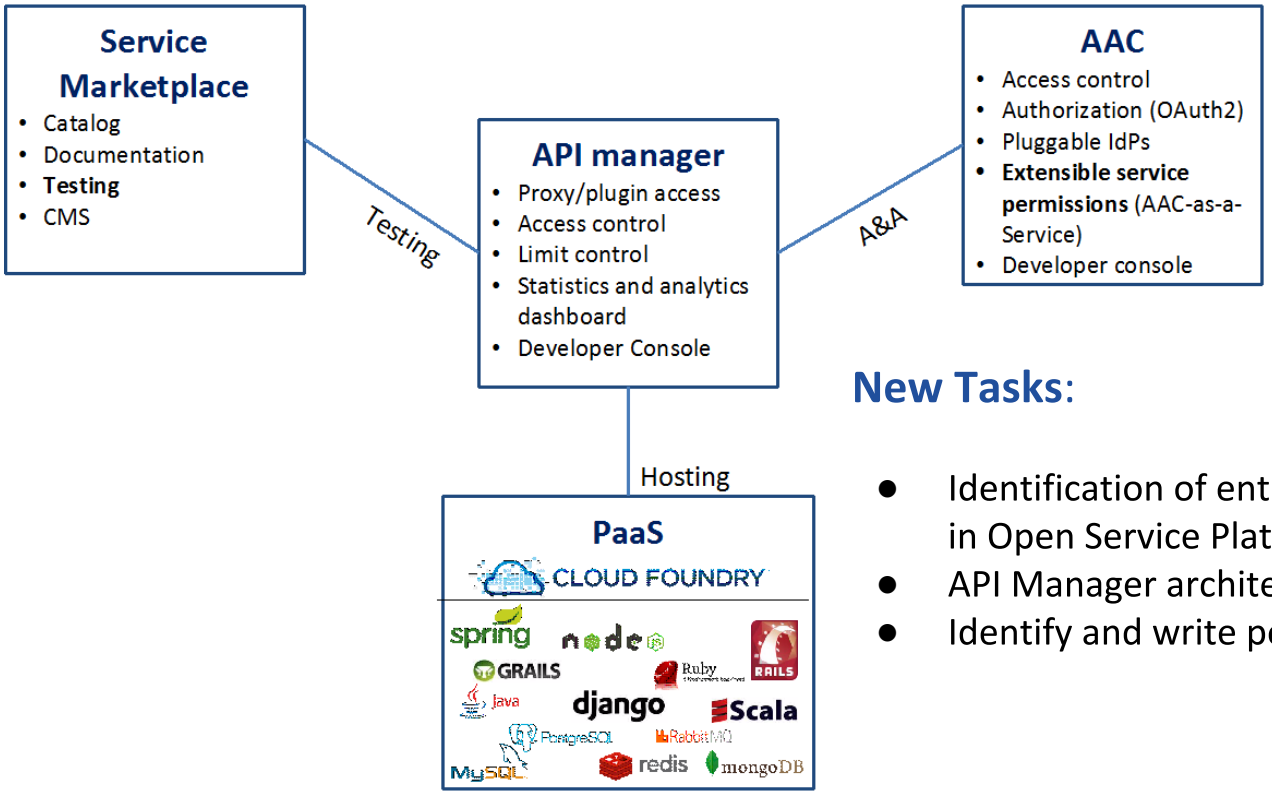
Solution





Flow \ Client Type	Public		Confidential
	Mobile	User-Agent Based	Web
Authorization Code	smart campus		smart campus
Implicit		smart campus	
RO Credential	smart campus		
Client Credential			smart campus

First SmartCampus Security Issue



New Tasks:

- Identification of entities and roles in Open Service Platform
- API Manager architecture model
- Identify and write policies

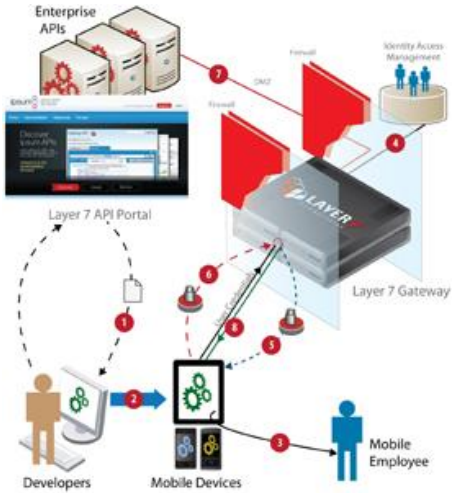
SC Open Services Platform

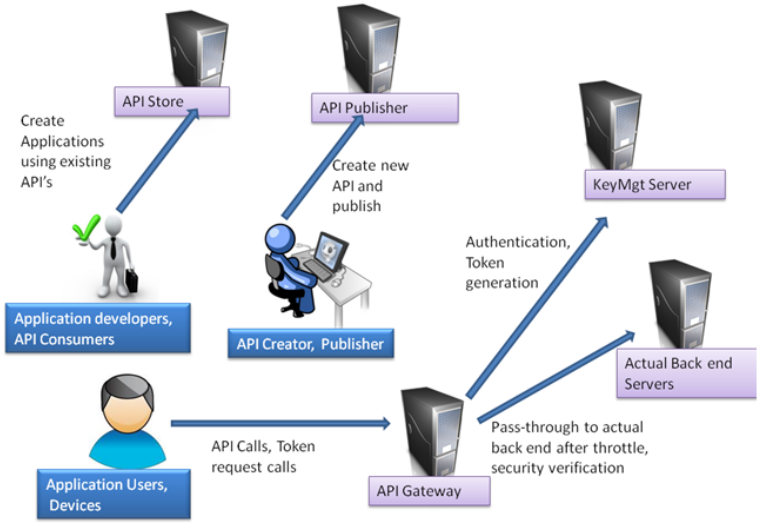
LAYER 7 TECHNOLOGIES
a CA Technologies company

MASHERY
An Intel Company

apigee

3SCALE

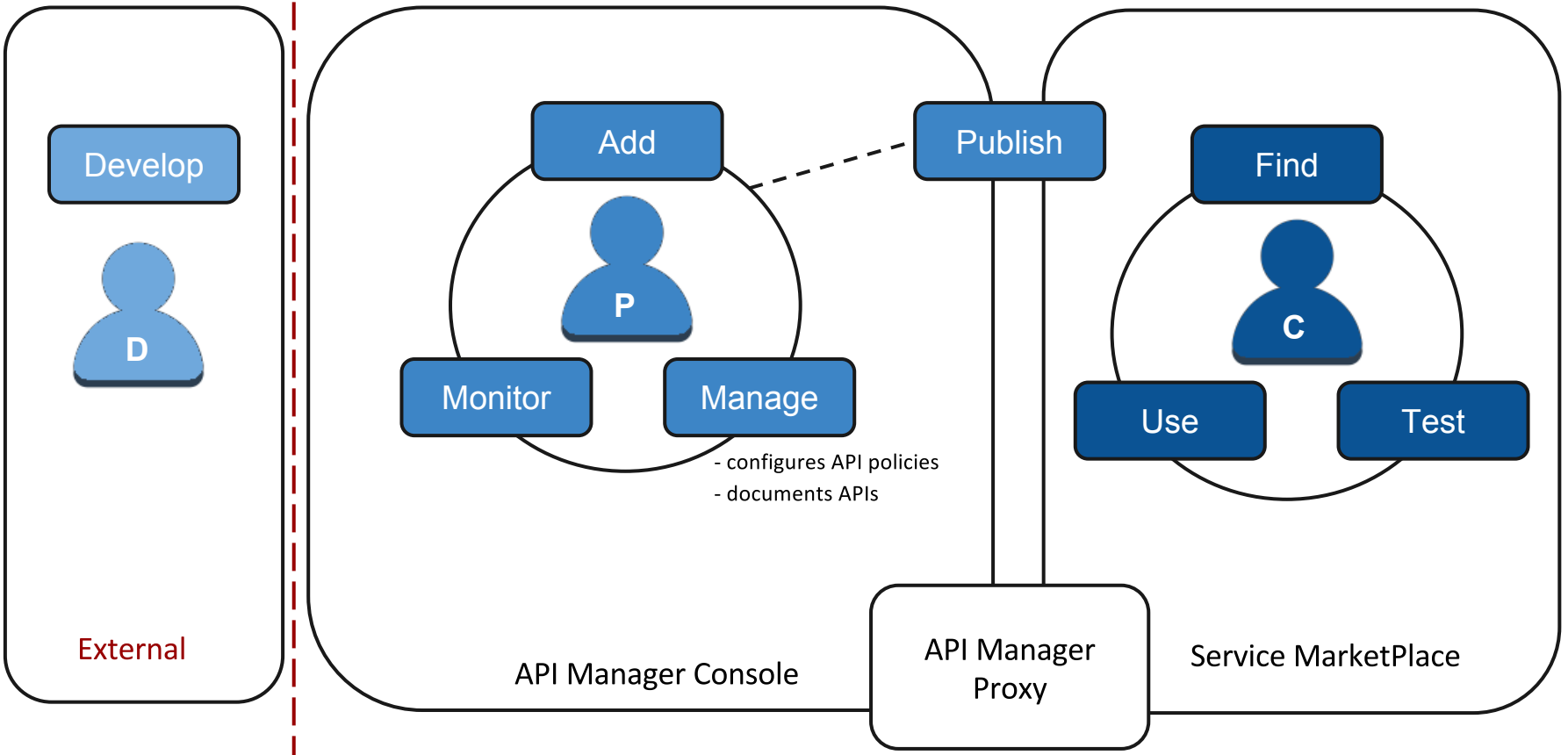




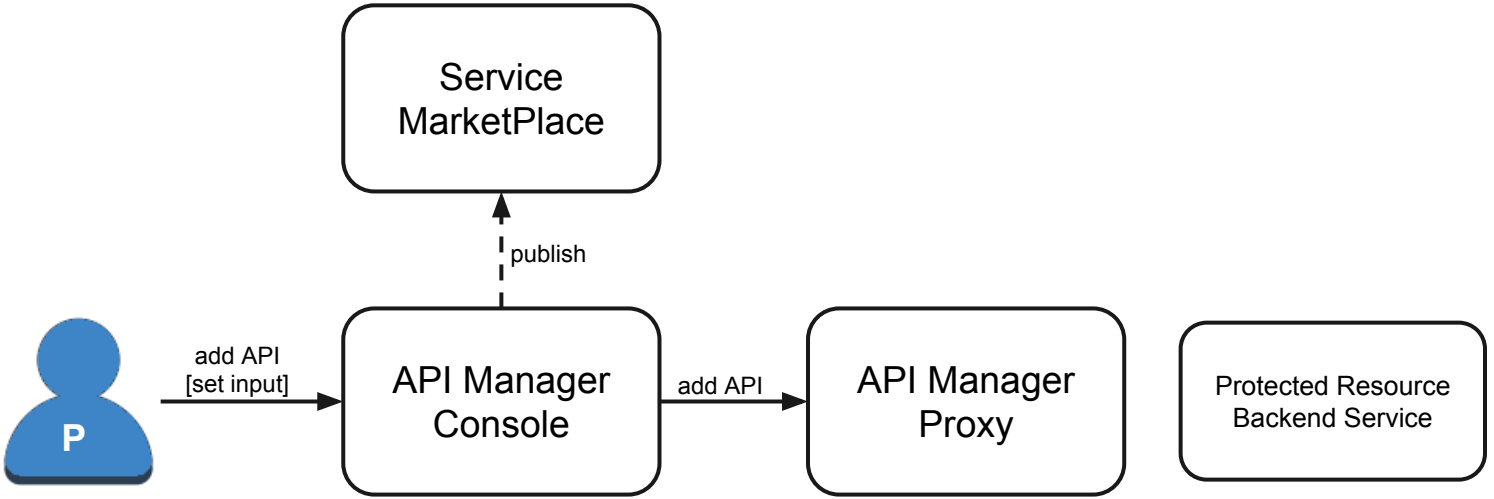
WSO2 API Manager

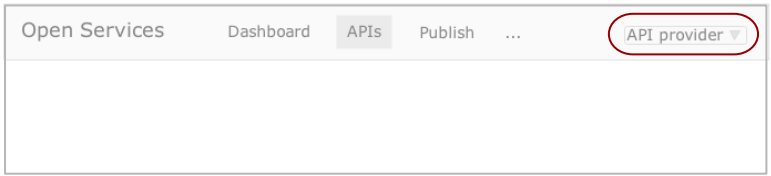
ApiAxle

API Manager Solutions

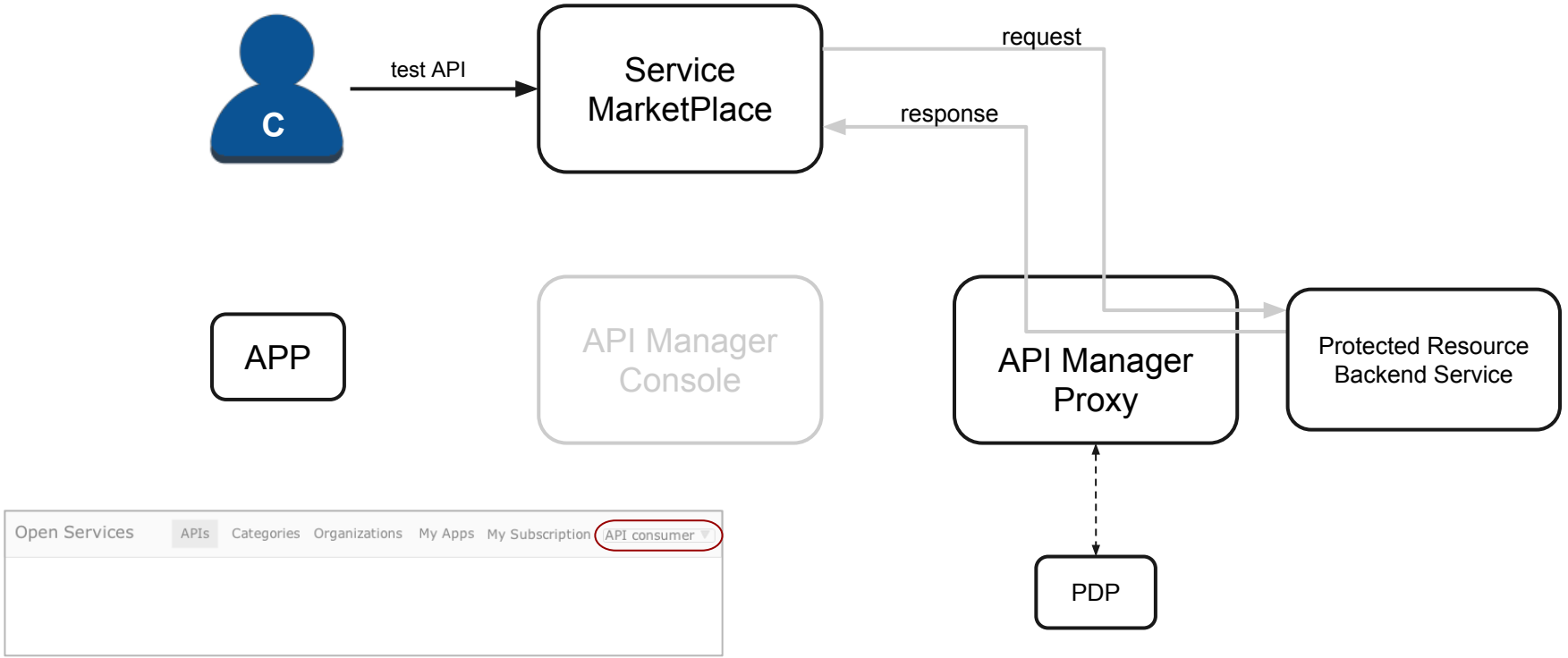


API Manager Roles





API Manager Components - API Provider



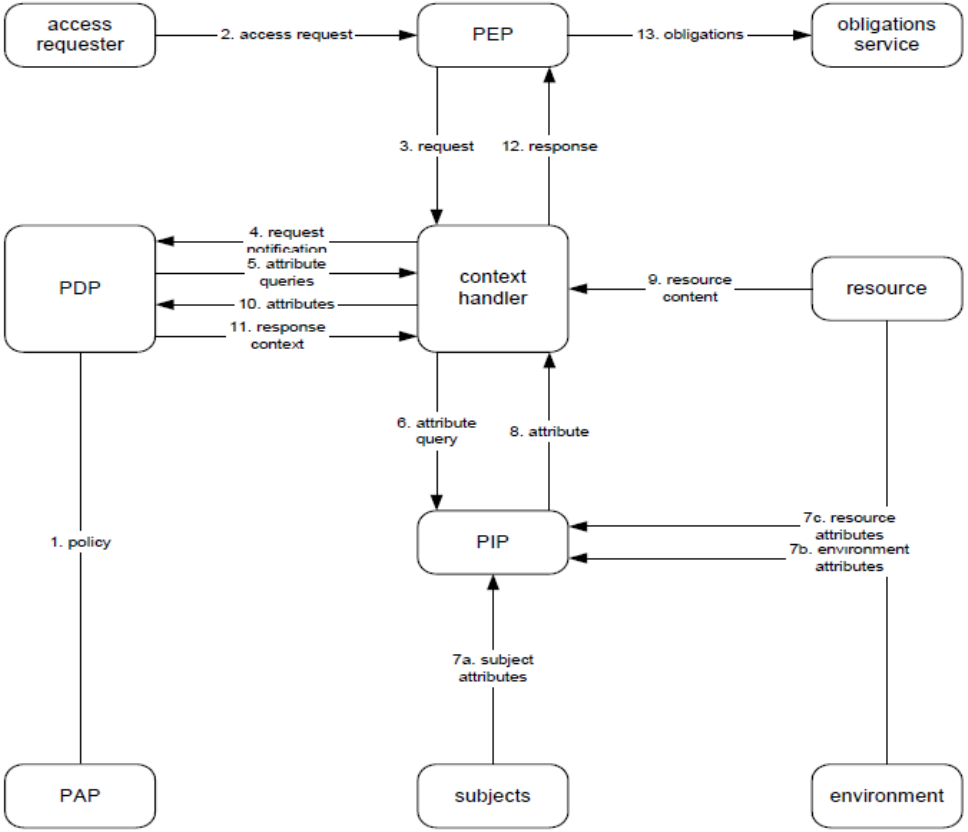
API Manager Components - API Consumer

Policy Administration Point (**PAP**) : the system entity that creates a policy or policy set

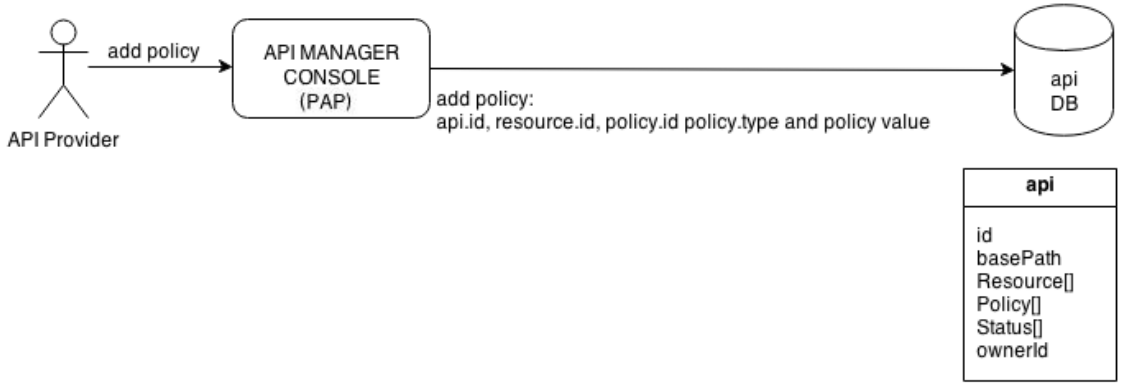
Policy Decision Point (**PDP**): the system entity that evaluates applicable policy and renders an authorization decision.

Policy Enforcement Point (**PEP**) : the system entity that performs access control, by making decision requests and enforcing authorization decisions.

Policy Information Point (**PIP**): the system entity that acts as a source of attribute values

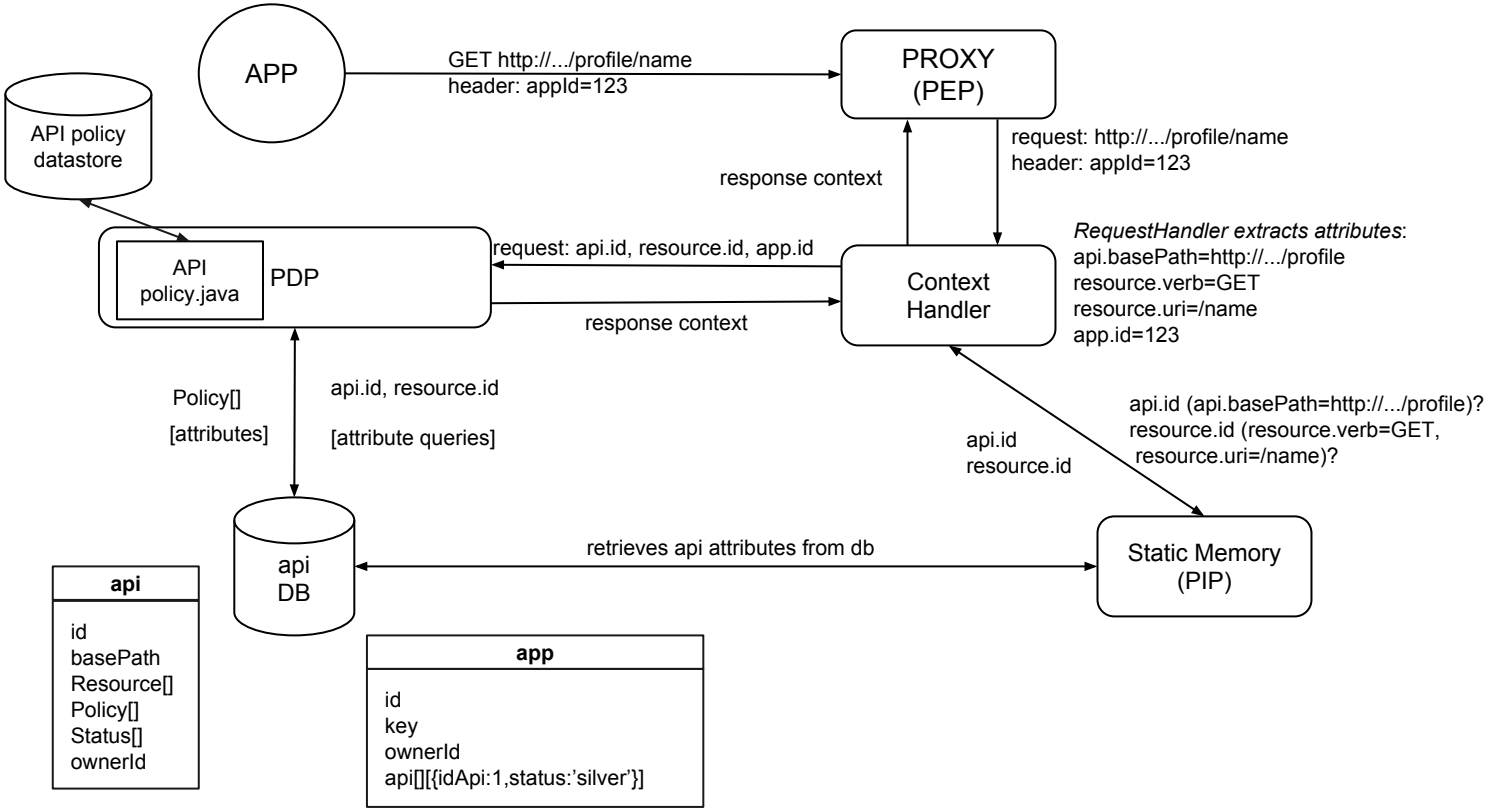


API Manager Architecture - XACML




```
{ "id" :10,
"basePath" : "/profile/name",
"resource" : [ ],
 "policy" : [ { "id" : 1, "spike-arrest-Rate" : "12pm", "type" : "SpikeArrest"},
            { "id" : 2, "quota-interval" : 1, "quota-TimeUnit" : "hour", "quota-Allow count" : 3, "qstatus" : [ {
            "name" : "Premium", "quota" : 6 }, { "name" : "Gold", "quota" : 5 } ], "type" : "Quota"} ],
 "status": [ { "name" : "Premium" }, { "name" : "Gold" } ] ,
 "ownerId" : "1"}
```

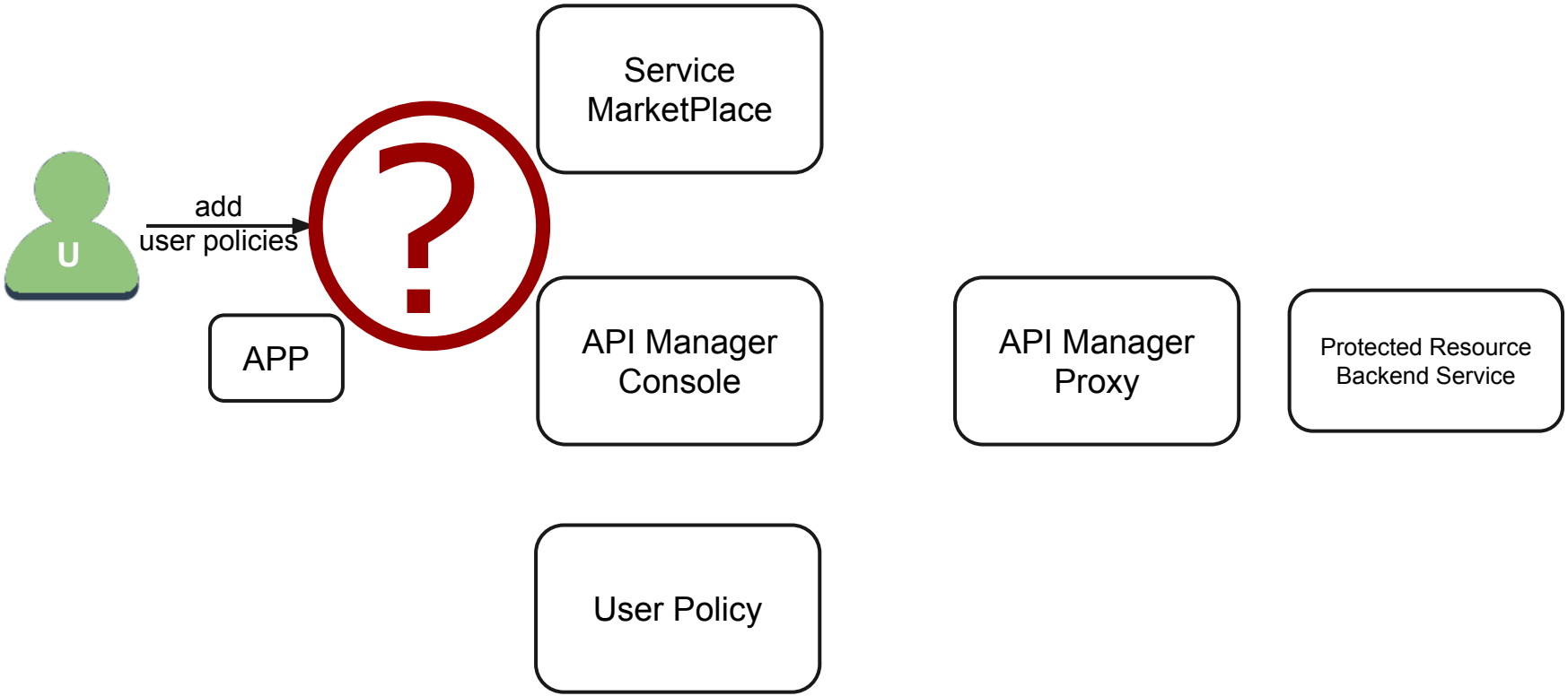
API Manager Architecture - add policy



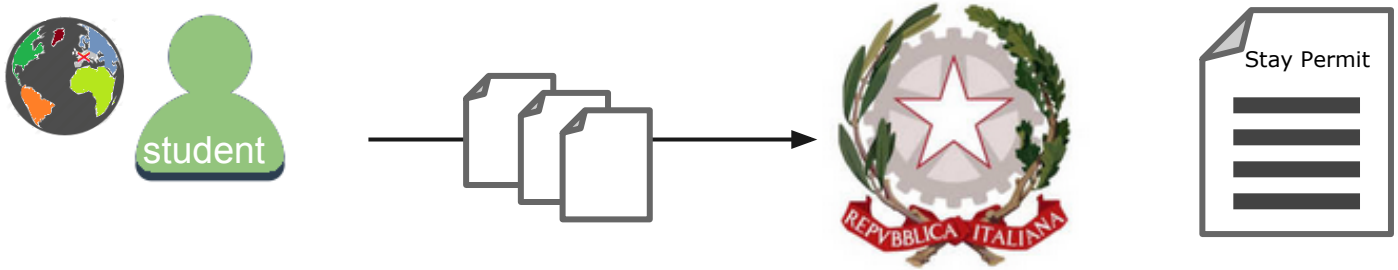
API Manager Architecture - API call

Policy Category	Description	Policy Name
Quality of Service	Rate Limit	Spike Arrest
Quality of Service	Rate Limit	Quota
Security	Access Control	IPAccessControl
Security	Access Control	VerifyAppKey
Security	Authorization	OAuth2.0
Security	Authentication	SAML

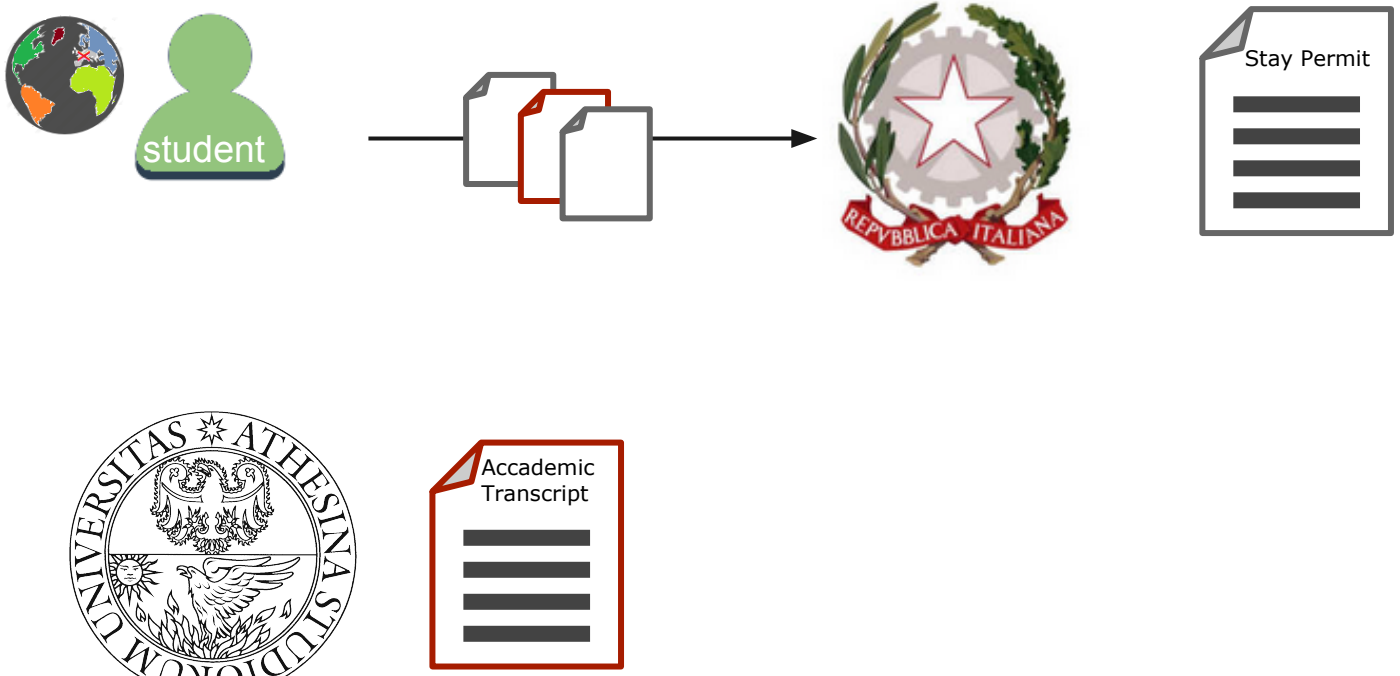
API Manager Policies



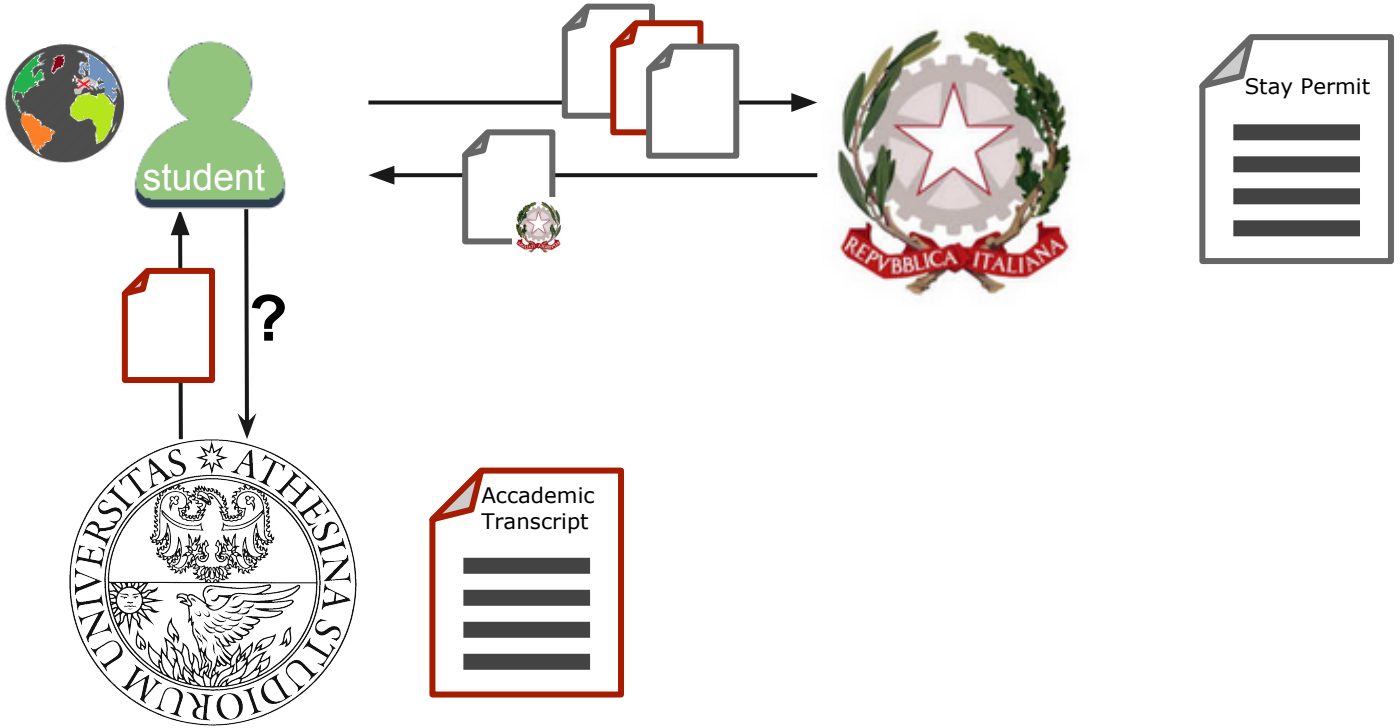
API Manager and User Policy (Silvio,Hari)



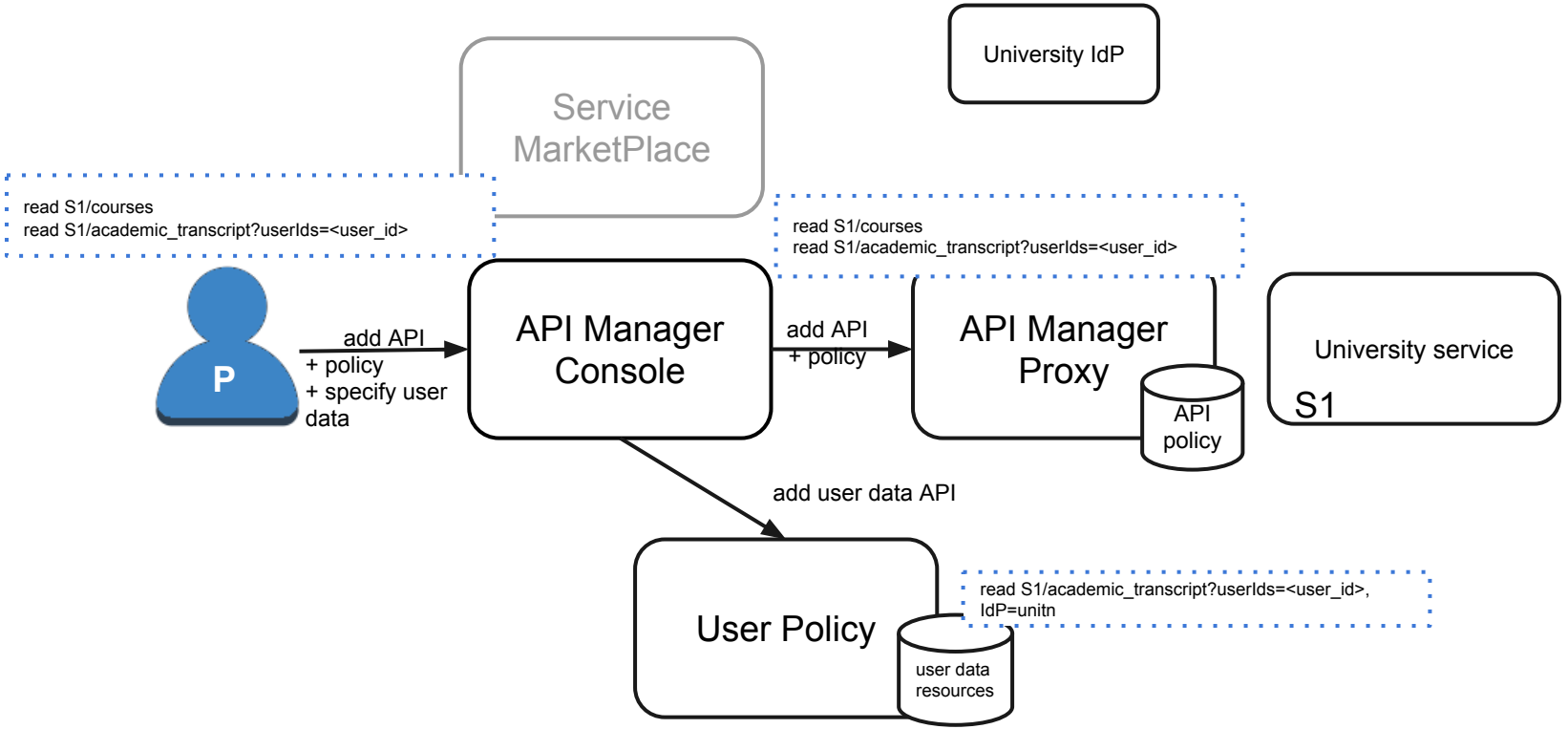
Use case: Foreign Student Stay Permit Renewal



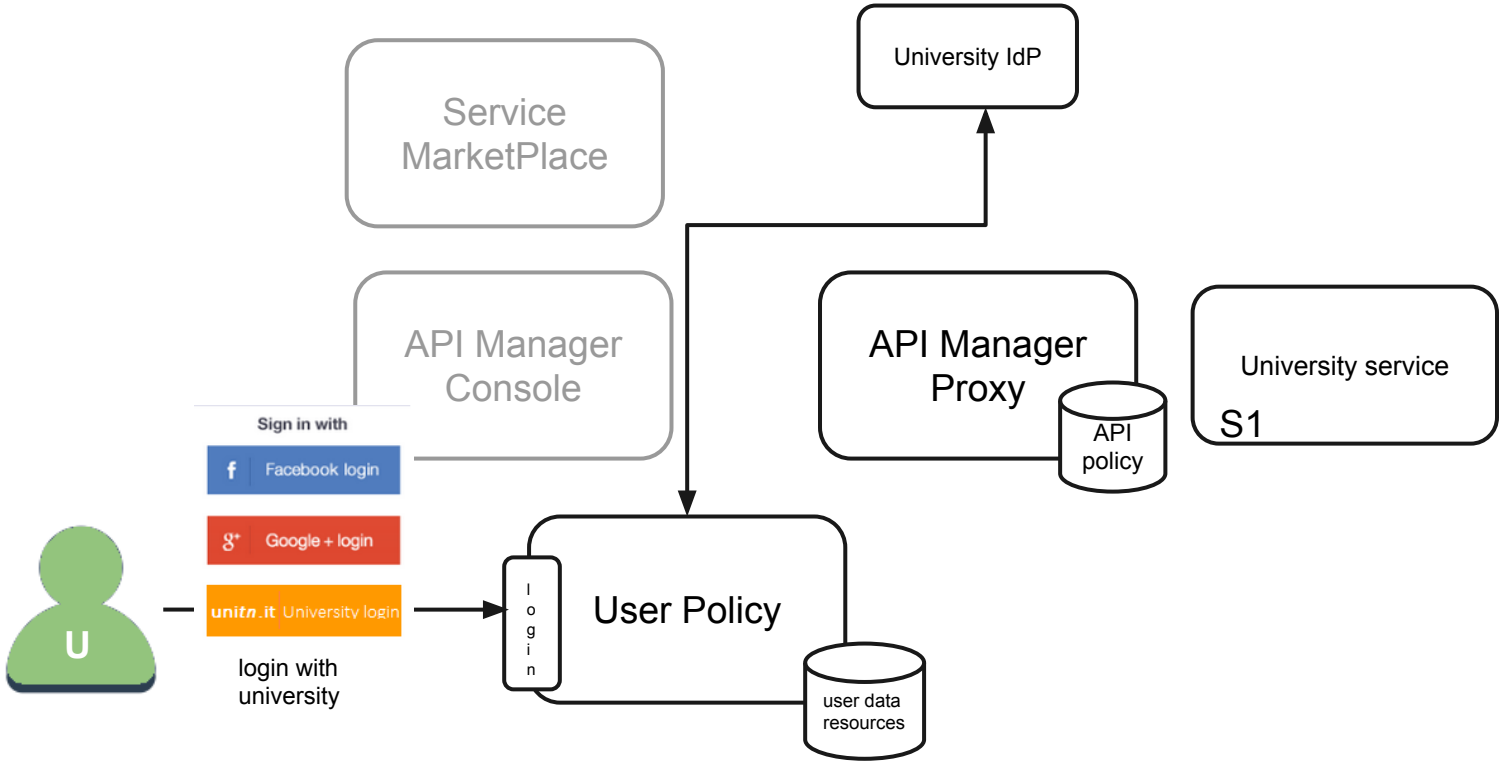
Use case: Foreign Student Stay Permit Renewal



Use case: Foreign Student Stay Permit Renewal

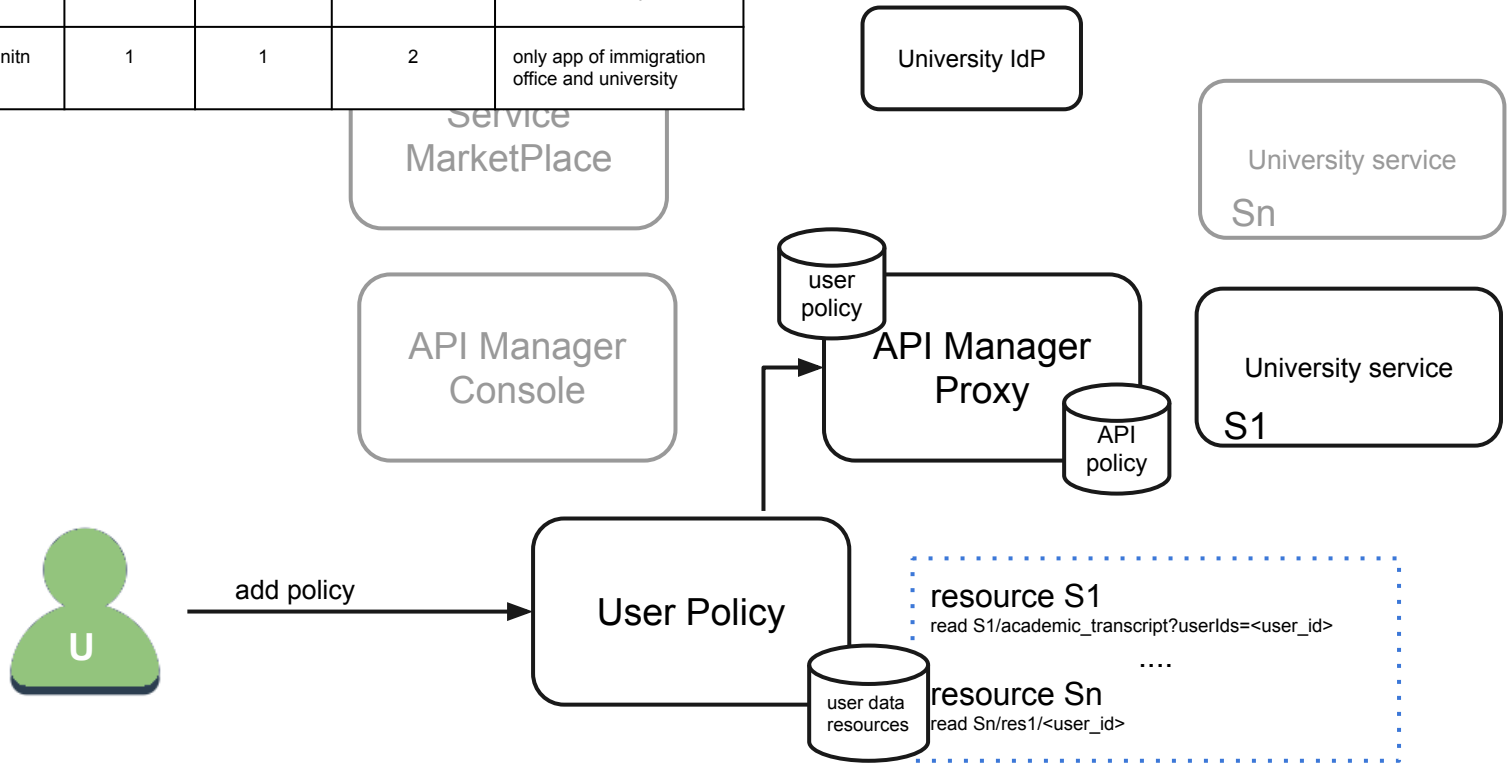

University IdP
Service MarketPlace
read S1/courses
read S1/academic_transcript?userIds=<user_id>
read S1/courses
read S1/academic_transcript?userIds=<user_id>
P
add API
+ policy
+ specify user data
API Manager Console
add API
+ policy
API Manager Proxy
API policy
University service
S1
add user data API
User Policy
user data resources
read S1/academic_transcript?userIds=<user_id>, IdP=unitn

Example


University IdP
Service MarketPlace
API Manager Console
API Manager Proxy
API policy
University service
S1
Sign in with
Facebook login
Google + login
unitn.it University login
U
login with university
login
User Policy
user data resources

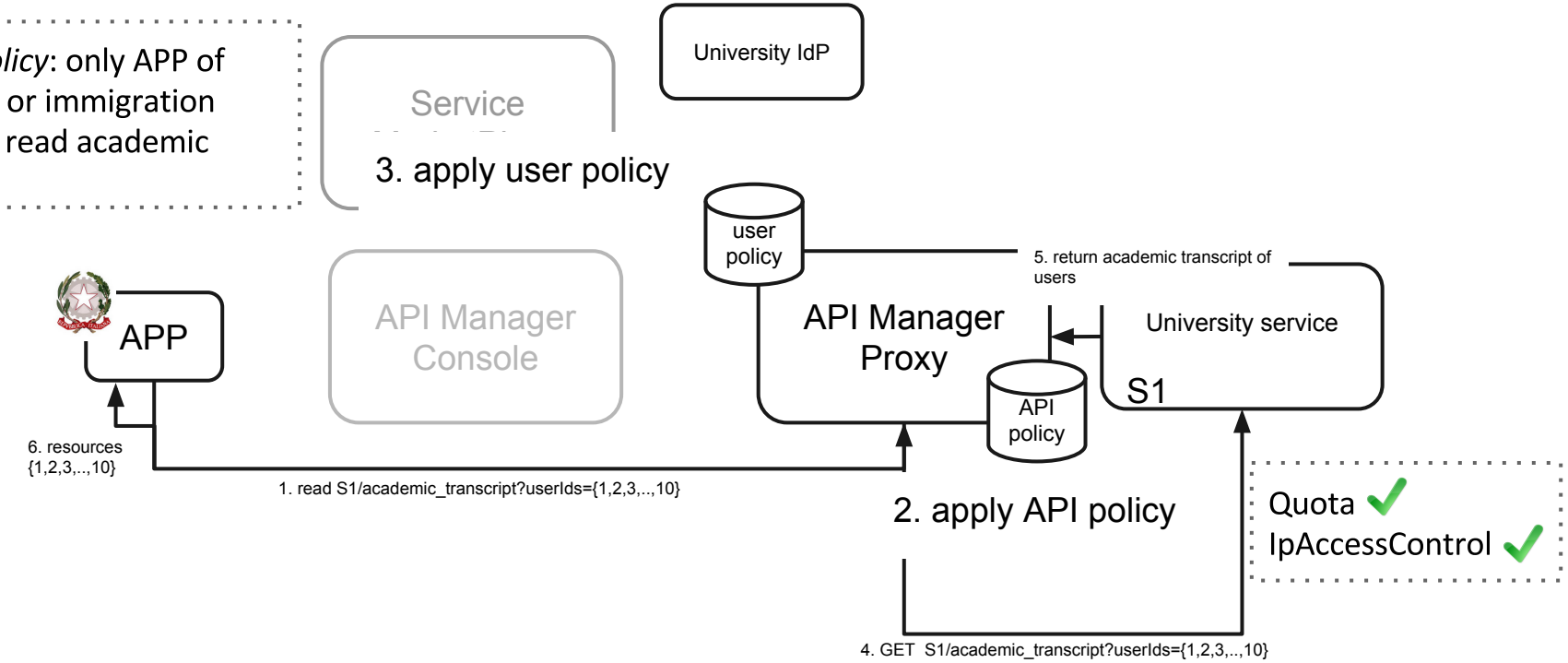
Example

IdP	user id	API id	resource id	policy
unitn	1	1	2	only app of immigration office and university



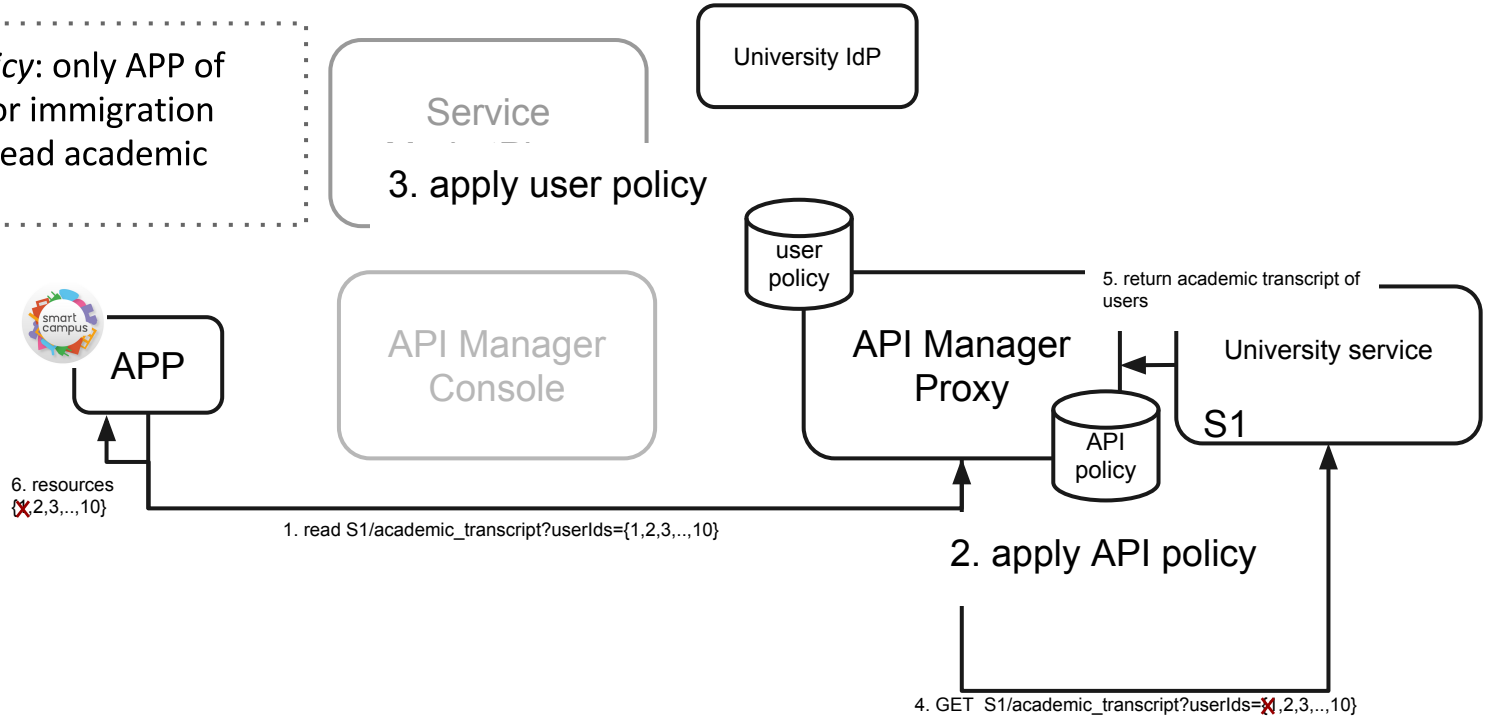
Example

USER 1 policy: only APP of university or immigration office can read academic transcript



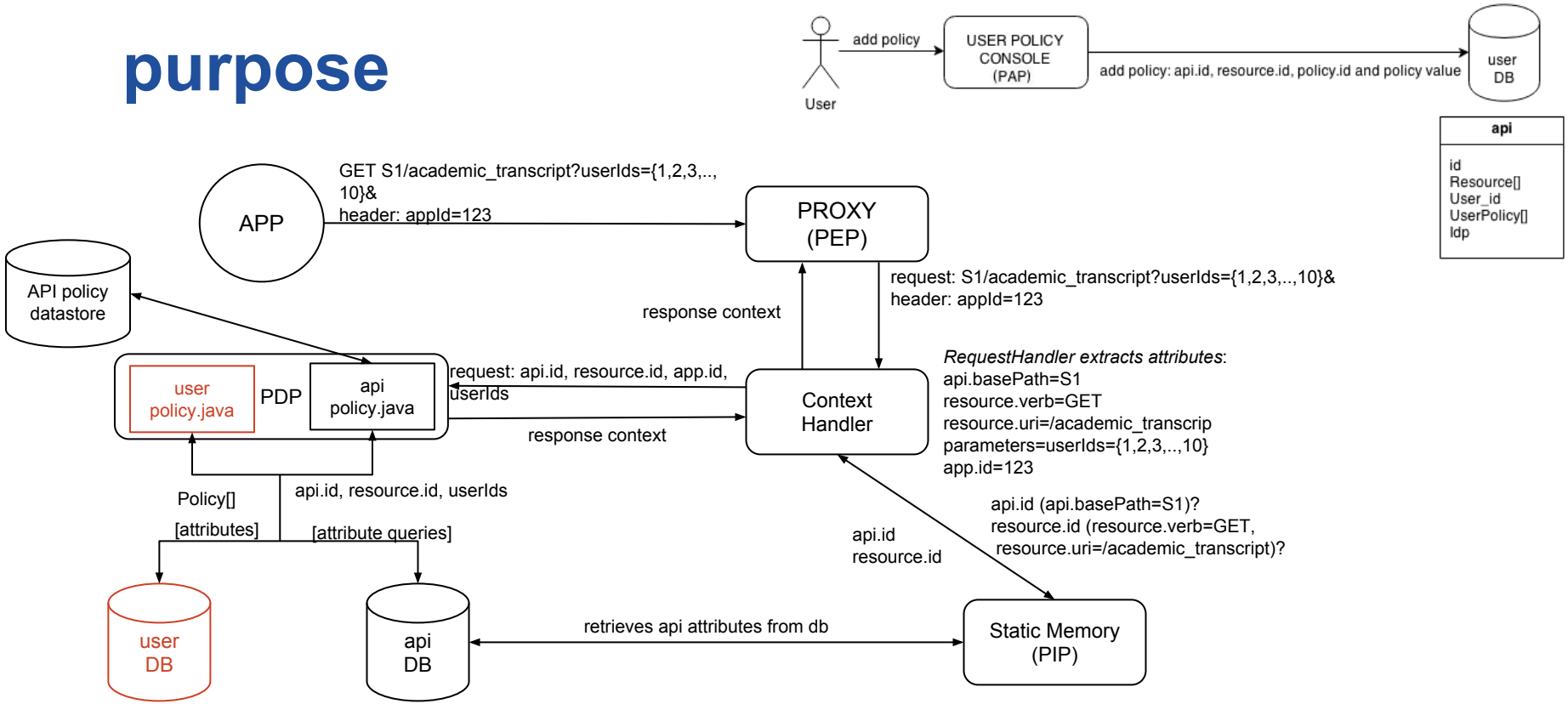
Example

USER 1 policy: only APP of university or immigration office can read academic transcript



Example

purpose



API Manager Architecture 2

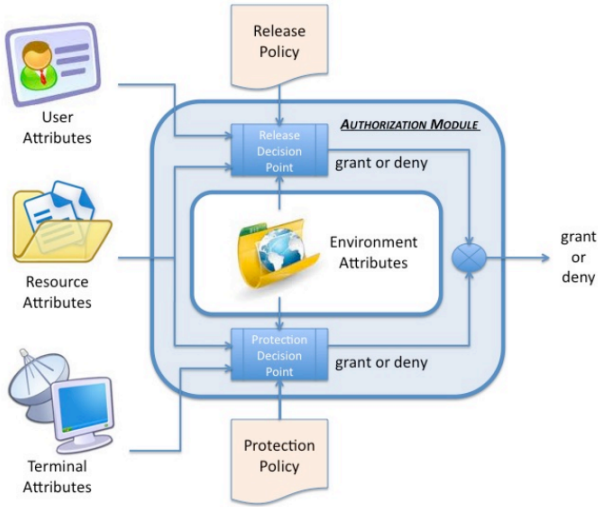
Two main goals:

1. extend the Content-based Protection and Release (CPR) tool for the NATO information sharing infrastructure to API Manager scenario. In particular, we want to create an approach to generate test inputs and automate the API Manager policies validation.

2. generalize the new version of the tool to a generic Attribute Based Access Control (ABAC) case

What is the CPR tool?

- CPR tool is used to specify and enforce access control policies that arise in organizations such as NATO.
- builds upon ABAC
- the designers express release and protection policies in a natural way using CPRL, that is a language based in the Satisfiability Modulo Theories (SMT) framework.



CPR Tool Extention and Test Case Generation (Silvio,Riccardo)

to extend CPR tool we have to:

- identify types, entities and attributes in API Manager scenario

```
entity APP = [ id:string, key:string, status: Status_value, ip_bv:(_Bitvector 32), apiList: IntList];
entity API = [ id:API_identifier];
entity Resource= [ id:string];
entity Request =[API_id:API_identifier, res_id:string, appKey=string, appId=string, OAuthToken: string, SAMLResponse:string];
....
```

- rewrite API provider rules and policies in the new language

```
entity Quota = [count: nat];

abstract rule Quota(s: Status_value, c:nat) {
        (APP.status =s && Quota.count <= c)
}
```

Starting point

Thanks for your attention!