
 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0.	Pàg. 1 / 23

MANUAL DE SEGURETAT


**Paradigma de seguretat en l'àmbit de
la publicació i consum d'APIs**

v1.0

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: <i>1.0</i>	Pàg. 2 / 23

Í N D E X

INTRODUCCIÓ	3
Objecte	3
Abast	4
DESCRIPCIÓ DE LA SOLUCIÓ	5
Actors involucrats	6
Tasques	6
Model de seguretat	12
Model de rols/permisos establerts	13
Configuració	14
Conclusions	15
Annex	15

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 3 / 23

1. INTRODUCCIÓ

En les dues seccions següents es fa un exercici a mode de resum executiu de tots els aspectes que formen part de la disciplina de configuració i aplicació del paradigma de seguretat establert pel servei de l'API Manager Transversal de CTTI.


1.1. Objecte

El model de seguretat i la seva aplicació és una activitat transversal dintre dels objectius de la present iniciativa. Els principals objectius del model de seguretat que s'ha definit són:

- Poder **publicar APIs de forma segura** garantint, en tot moment, l'accés a les mateixes alhora que es manté la integritat i la seguretat dels backoffices que exposin els seus serveis/operacions/dades mitjançant la solució API Connect és un dels objectius clau del projecte de l'API Manager.
- Poder **oferir de forma segura, ben gestionada i auditable**, la possibilitat a la ciutadania i als àmbits de la Generalitat i altres organismes relacionats, **el consum d'APIs publicades** que poden esdevenir fonts comunes d'operacions i d'informació.
- **Establir la configuració, les fonts d'usuaris de confiança i els diversos graus d'accés** (rols/ permisos) **a les diverses eines tecnològiques** que s'empraran en aquesta iniciativa (SaaS IBM API Connect, on-Premise IBM API Gateways, SaaS IBM Portals dels 4 catàlegs, KeyCloak Gicar/Corporatiu i KeyCloak/Justícia) és un dels aspectes claus que tracta el document.
- **Establir les polítiques de publicació de les APIs** i, en concret, forçar que tots els plans de consum tinguin la obligatorietat de l'aprovació de les sol·licituds de subscripció a les APIs esdevindrà un dels instruments de control bàsics i principals que ens facilitin la gestió i el coneixement, en tot moment, de les fonts de consum de les APIs publicades i el seu grau de consum (item important per a aspectes de facturació del consum d'una API publicada).
- **Permetre als responsable del servei Cloud / CTTI i el responsable de l'àmbit / codi de diàleg publicador (d'APIs) prendre decisions com ara revocar subscripcions i/o bloquejar consum inapropiats de certes APIs** també és una funcionalitat rellevant i que està íntimament emparentada amb la implantació del model seguretat establert pel projecte.

Tots els paràgrafs anteriors componen, a grans trets, les necessitats de seguretat associades a la present iniciativa.

Aquest document aporta les respostes a les qüestions sobre el "què i el com" ho farem.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 4 / 23

1.2. Abast


Estructurem el present document incidint en els aspectes claus relatius a l'aplicació del model de seguretat i la seva utilització per a tots els actors involucrats:

- **Actors involucrats (perfils):** Es descriuen tots els actors involucrats en tots els aspectes relacionats amb el servei de publicació i consum d'APIs.
 - CTTI.
 - Oficina tècnica API Manager Transversal.
 - Proveïdors de nous gateways on-premise dedicats, publicadors d'APIs, consumidors d'APIs.
 - Usuaris publicadors d'APIs (d'un codi de diàleg).
 - Usuaris dels portals de consumidors d'APIs (un portal per a cada catàleg).
 - Usuaris finals (corporatius o externs) que utilitzin SPAs i/o altre programari que inclou el consum d'una API amb protecció d'accés addicional del tipus KeyCloak(Corporatiu) i/o protecció d'accés del tipus KeyCloak(propri d'un departament).
 - Usuaris responsables en la facturació del consum de les APIs.

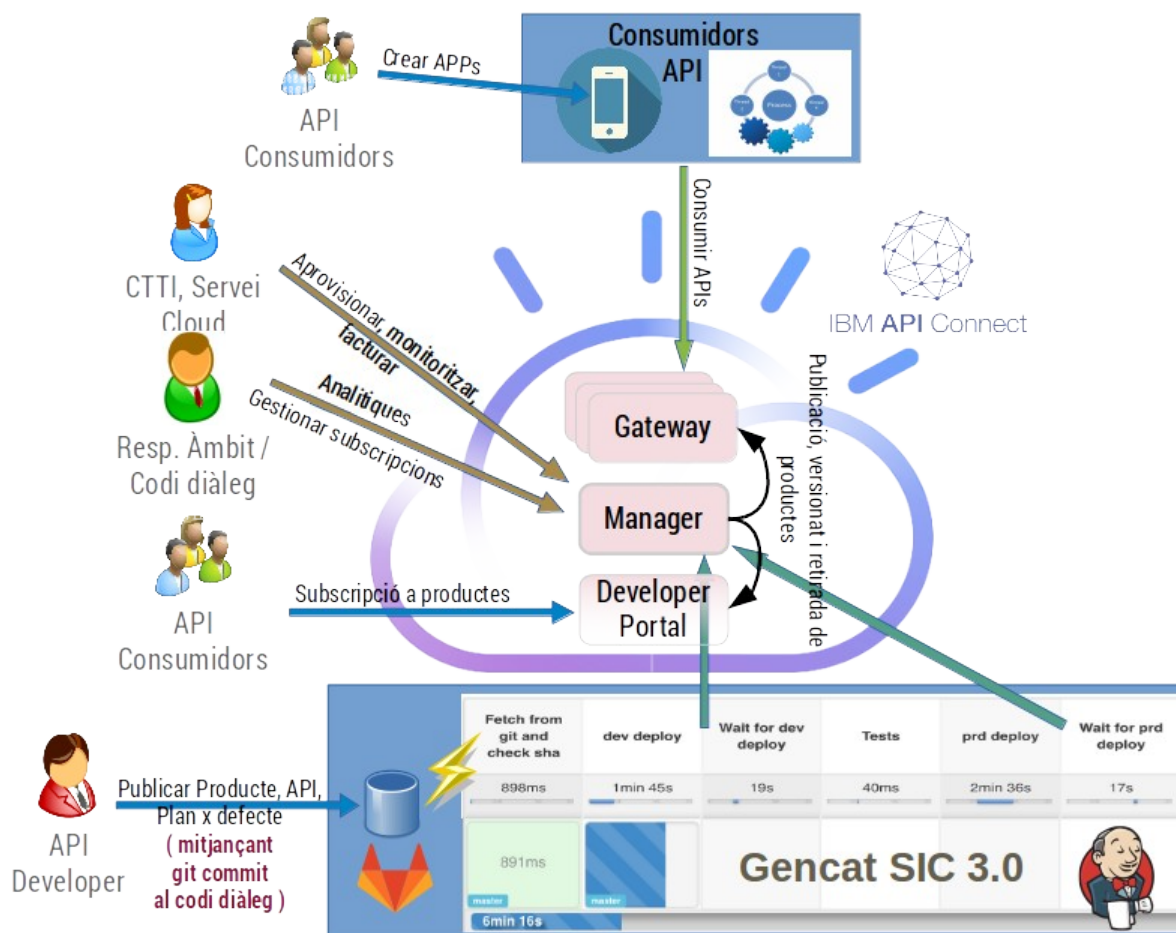
- **Eines/Serveis:** Descripció de les eines i funcionalitats que caldrà tenir en compte per a la gestió dels permisos associats a les mateixes.

- **Tasques/operatives:** Tasques identificades que estiguin subjectes a un o més mecanismes de seguretat. I que es componen d'un conjunt d'accions a dur a terme.

- **Accions identificades:** Tota tasca (operativa) està composta per una o més accions que cal portar a terme emprant una eina. Aquí és on s'incidirà en aspectes de configuració per a securitzar l'accés a aquestes accions dintre de les diverses eines que componen el parc tecnològic de la present solució.


	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 5 / 23

2. DESCRIPCIÓ DE LA SOLUCIÓ



Elements principals de la solució:

Element	Descripció
Gitlab SIC 3.0	Repositori de codi on els col·laboradors desaran la definició del fitxer aca i dels yamls de descripció d'un producte i de l'API que es publicarà
Jenkins SIC 3.0	Eina CI/CD amb la que el responsable del codi de diàleg (on es produeix l'API) pot dur a terme totes les operatives relatives al cicle de vida del binomi API (versió) - producte (versió)
API Connect	Programari SaaS d'IBM (desplegat al servei cloud públic d'IBM que permet fer totes les tasques de gestió addicionals incloses en la gestió del cicle de vida del binomi api (versió) - producte (versió)
API Gateway (on-Premise)	Gateway de servei encarregat de controlar l'accés a les APIs

	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 6 / 23

	publicades i establir les comunicacions (i validar la seguretat) abans de passar les peticions als backoffices involucrats i destinataris finals de les operacions que es publiquen a API Connect
Portal del desenvolupador (per catàleg)	Per a cadascun dels catàlegs aprovisionats es crea un portal per posar a disposició dels usuaris (futurs consumidors dels productes publicats sota els espais CD < codis de diàleg >) la possibilitat de subscriure's al consum de les APIs

2.1. Actors involucrats


En les diferents eines participen diversos tipus d'usuaris/perfils:

Nom	Descripció
CTTI	Àmbit Generalitat responsable del servei d'API Manager
OT API Manager (Usuari Suport Cloud)	Responsable del suport i l'operació de la plataforma
Àmbit	Responsable de totes les APIs que es publiquen sota el seu patrocini
Release Manager CD	Release manager associat a un codi de diàleg. Mitjançant l'auto-aprovisionament poden donar permisos als usuaris desenvolupadors sobre els pipelines que s'aprovisionen per a cada CD i sobre el repositori del Gitab associat al CD
API developer	Usuaris Gencat amb permisos al Gitlab/SIC per a l'execució de pipelines i del desplegament de les APIs
API consumidor	Release Manager/developers associats a un CD responsable del consum d'una o N APIs publicades
CPD2/IBM	Responsable de l'aprovisionament i la gestió de tots els gateways que formen part de la plataforma


2.2. Tasques

A continuació es mostren les tasques que requereixen de gestió de permisos:

Activitats a realitzar			Permisos involucrats			
Disciplina	Acció	Eina/ automatisme/ sub-acció	Fase 0 - Oficina Tècnica APIM/SIC	Àmbit	Release Manager	Developer


 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 7 / 23

Desenvolupar / Publicar APIs						
	Preparar projecte publicació d'APIs		<p>Crear el gitlab associat al CD.</p> <p>Crear el fitxer aca.yml dins del repo.</p> <p>Crear els pipelines associades al CD.</p> <p>Assignar permisos al responsable d'àmbit i al release manager per a que puguin gestionar els usuaris del projecte al GitLab.</p> <p>Assignar permisos al release manager per a que pugui executar les pipelines associades al CD.</p> <p>Aprovisionar el CD als catàlegs pertinents i afegir els permisos pel responsable d'àmbit i el release manager del CD.</p>			
	Crear API / Producte	Instal·lar toolkit local a l'ordinador dels desenvolupadors				Permisos per a instal·lar el toolkit gratuït de l'API Connect en l'ordinador local
	Entregar API / Producte	SIC/Gitlab Pujar al Gitlab la		Validar accés al gitlab	Assignar permisos als usuaris	Validar que pot pujar i fer commit


	API Manager - Manual de seguretat		N. revisió doc.: 1.0	
	Manual d'usuari			
	N. versió solució: 1.0		Pàg. 8 / 23	

		definició del producte / api com a ymls		associat al codi de diàleg	desenvolupadors per a poder fer commit al gitlab associat al codi de diàleg (en modalitat autogestió de projectes)	al repositori del gitlab associat al codi de diàleg
	Publicar Producte	<p>SIC / Pipeline Jenkins</p> <p>Execució del pipeline de publicació del producte:</p> <ul style="list-style-type: none"> - substitució de la configuració del plà de subscripció (forçant l'aprovació de les subscripcions futures) - substitució de la configuració de seguretat i incorporar la referenciada al fitxer aca.yml 		Validar els permisos d'execució dels jobs al jenkins	<p>Validar els permisos d'execució dels jobs al jenkins</p> <p>Executar el pipeline de publicació al jenkins</p>	Permisos de lectura per a veure el resultat de l'execució dels jobs
	Gestió del Cicle de Vida del Producte	SIC / Pipeline Jenkins		Validar els permisos d'execució dels jobs al jenkins	Executar els pipelines associats a la gestió del cicle de vida del producte	Permisos de lectura per a veure el resultat de l'execució dels jobs


Consum d' APIs						
	Subscripció al portal de consum d'APIS	Portal de consum d'APIS				L'usuari executa l'acció d'autoregis

	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 9 / 23


	(veure manual de consum d'APIs)					tre als portals involucrats
	Creació d'una APP consumidora de Productes	Portal de consum d'APIs				L'usuari crea tantes APPs com necessiti per a fer el consum d'APIs (productes) Cada App té associat el seu clientID
	Subscripció a un producte	Portal de consum d'APIs				L'usuari sol·licita selecciona la subscripció a un producte publica t i el vincula a una de les seves Apps (clientID)
	Aprovació de la subscripció d'una producte	API Connect (SaaS)	L'equip de suport de l'oficina tècnica d'APIM (previa aprovació del responsable d'àmbit del producte publicat), entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i accepta subscripció	El responsable d'àmbit del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/es	El release manager del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/es	L'usuari reb mail de confirmació de l'acceptació de la subscripció El producte passa a estar operatiu al gateway associat al catàleg/es pai a on està publicat el

	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 10 / 23

				paï pertinent i accepta la subscripció	pertinent i accepta la subscripció	producte
Denegació de la subscripció d'un producte	API Connect (SaaS)	L'equip de suport de l'oficina tècnica d'APIM (previa decisió del responsable d'àmbit del producte publicat), entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i rebutja subscripció	El responsable d'àmbit del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i rebutja la subscripció	El release manager del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i rebutja la subscripció	L'usuari rep mail de denegació de l'acceptació de la subscripció. Es rebutja la subscripció al producte.	
Eliminació de la subscripció d'un producte	API Connect (SaaS)	L'equip de suport de l'oficina tècnica d'APIM (previa decisió del responsable d'àmbit del producte publicat), entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i elimina la subscripció	El responsable d'àmbit del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i elimina la subscripció	El release manager del producte publicat rep email amb la sol·licitud de descripció. Entra a l'eina API Connect (SaaS), s'adreça al catàleg/espai pertinent i elimina la subscripció		

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 11 / 23

Operació de la plataforma						
	Configuració proveïdor OAUTH2 (KeyCloak)	API Connect SaaS/SIC 3.0	<p>L'oficina tècnica amb el proveïdor dels servei d'OAUTH2 a incorporar, realitzarà la configuració del nou proveïdor d'OAUTH2 a API Connect.</p> <p>S'autoritza l'ús del nou servei OAUTH2 a tots els catàlegs i al catàleg de "Sandbox".</p> <p>Es modifiquen les plantilles del SIC 3.0 (d'aprovisionament de pipelines per a custòdia l'snippet de codi i les urls < endpoints > associats al nou proveïdor.</p> <p>Dintre del fitxer aca.yml es pot passar a seleccionar l'àlies associat al nou proveïdor de seguretat OAUTH2 com a font de validació</p>			<p>L'usuari client de l'API és el responsable de programar l'enviament , a les peticions, de la capçalera Authorization amb el token ("bearer") OAUTH2 que representa la identitat de l'usuari Gencat que està fent la petició a l'API protegida després d'haver-se identificat amb el SSO / OAUTH del proveïdor de seguretat (siqui aquest Gicar, Justícia o d'altres que s'integraran a</p>


	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 12 / 23

						posteriori)
	Instal·lar certificats	API Connect / API Gateway	To be defined	To be defined	To be defined	To be defined
	Registre Gateways a API connect	API Conect	Un cop el proveïdor (IBM) marca els gateways aprovisionats com a vàlids i els registres com a gateway disponibles a la solució, l'oficina tècnica passa a utilitzar els nous gateways al catàleg / CD < codis de diàleg > als que estan destinats			

3. Model de seguretat

Recordem els principals actors de la sol·lució

Nom	Descripció
CTTI	Àmbit Generalitat responsable del servei d'API Manager
OT API Manager (Usuari Suport Cloud)	Responsable del suport i l'operació de la plataforma
Àmbit	Responsable de totes les APIs que es publiquen sota el seu patrocini
Release Manager CD	Release manager associat a un codi de diàleg. Mitjançant l'auto-aprovisionament poden donar permisos als usuaris desenvolupadors sobre els pipelines que s'aprovisionen per a cada CD i sobre el repositori del Gitab associat al CD
API developer	Usuaris Gencat amb permisos al Gitlab/SIC per a l'execució de pipelines i del desplegament de les APIs
API consumidor	Release Manager/developers associats a un CD responsable del consum d'una o N APIs publicades
CPD2/IBM	Responsable de l'aprovisionament i la gestió de tots els gateways que formen part de la plataforma

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 13 / 23

3.1. Model de rols/permisos establerts

- Usuaris del “Rol CTTI”:

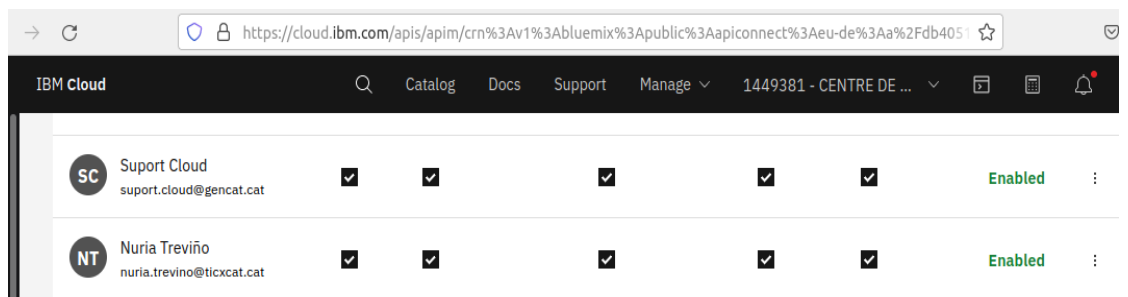
L'usuari CTTI atorga el rol de gestió d'usuaris del compte CTTI contractat al servei Cloud d'IBM als usuaris següents amb IBMid:

- Nuria Treviño.
- Joan Garcia.
- Suport Cloud.

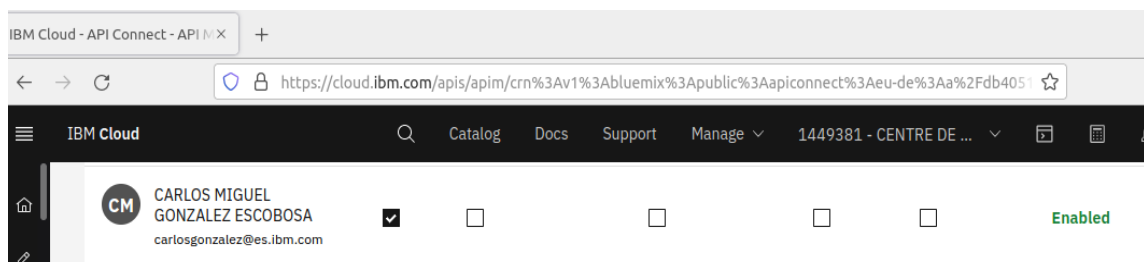
L'oficina tècnica ha de poder convidar a IBM API Connect (CTTI) als usuaris (amb rol) responsable àmbit o release manager en la fase 0 dels projectes (CDs) que vulguin disposar de la nova funcionalitat de desplegament d'APIs al API Connect.

L'usuari identificat amb rol CTTI tindrà assignat el Rol admin a totes les organitzacions, catàlegs i espais poden realitzar qualsevol acció disponible (actual i futura) del SaaS API Connect.


- Usuari “Support Cloud” (el que utilitza l'equip de l'OT API Manager):
 - Disposa de tots els rols d'API Connect a totes les organitzacions / catàlegs / espais i poden realitzar totes les activitats dins de l'eina API Connect relatives a l'organització, configuració de proveïdors de seguretat third-party OAUTH2, creació de noves organitzacions, catàlegs i espais.



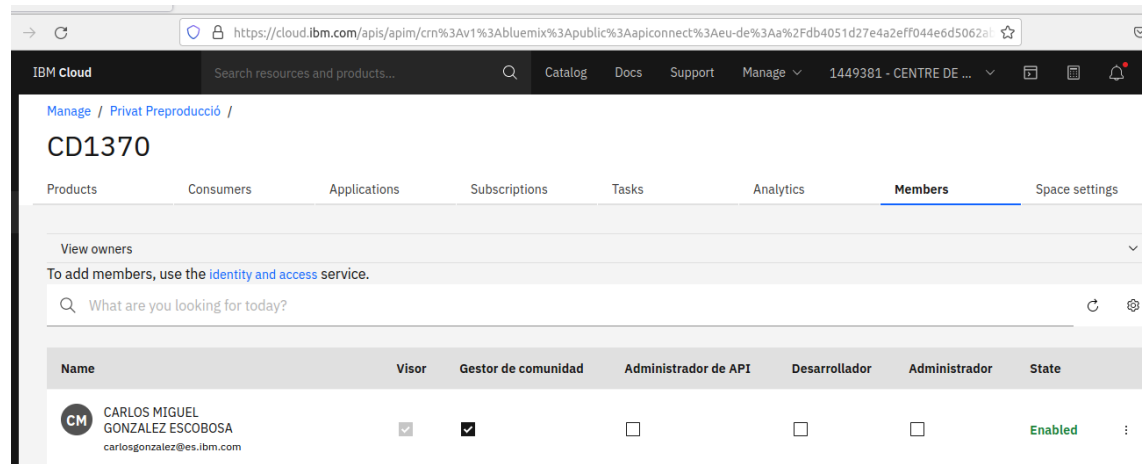
- Assigna el Rol API Connect “View / Visor “ a les organitzacions a tots els release managers / responsables d'àmbit. Aquest rol permet accedir als codis de diàleg a on tenen APIs/productes publicats.



- Dins del codi de diàleg pertinent CDXXXX, s'assigna el rol “Community manager” als responsables d'àmbit i al release manager del CD que publica APIs. Així poden

	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 14 / 23

accedir a les funcionalitats de gestió de les subscripcions i les analítiques de consums.



- Crear les invitacions a usuaris, amb IBMid, per a tenir accés a l'API Connect.

3.2. Configuració

3.2.1. Pla de consum amb subscripció

Tots els productes es publicaran, via SIC 3.0, i incorporaran el pla estàndard de consum que establirà:

- obligatorietat de compliment de les restriccions de nombre de peticions.
- límit dels nombre de peticions per minut (valor a consensuar amb CTTI).
- límit màxim (burst) de les peticions per segon (valor a consensuar amb CTTI).
- aprovació obligatoria.


3.2.2. Proveïdor KeyCloak/OAUTH2

Per a configurar un proveïdor extern de seguretat (OAUTH2) cal:

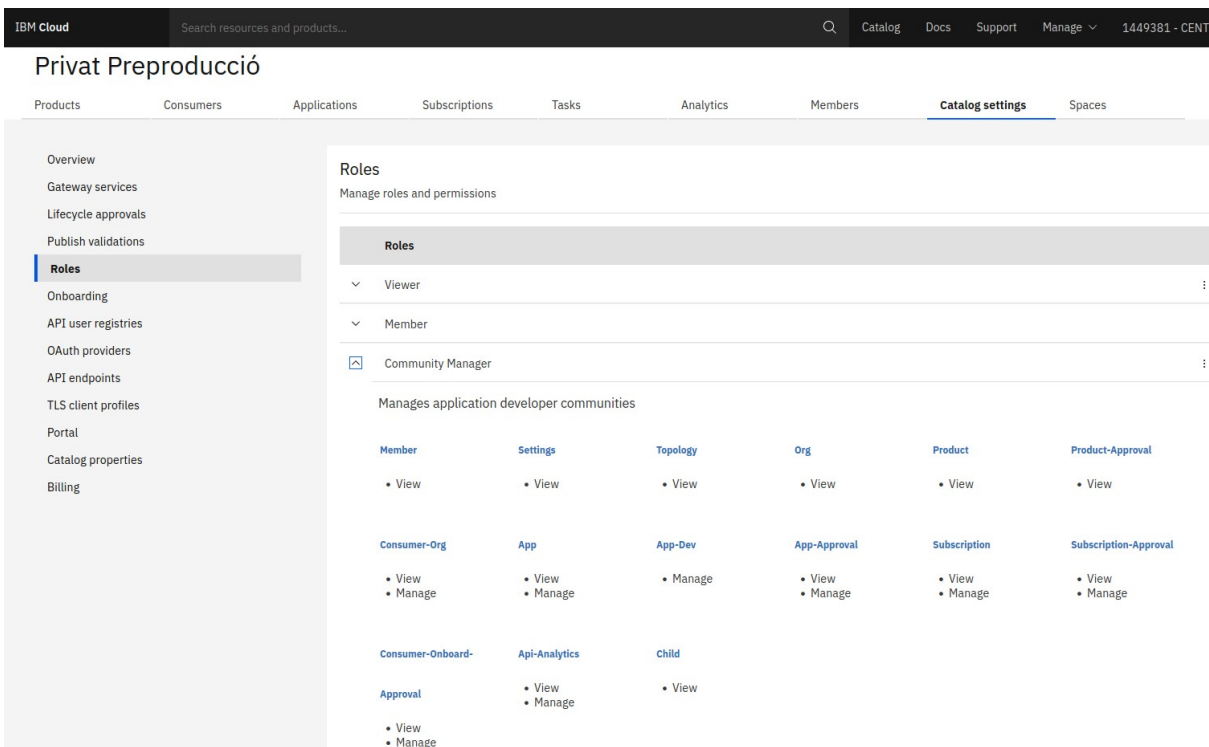
- Crear el proveedor.
- Associar-lo a tots els espais a on es sol·licita el seu ús.
- Associar-lo al catàleg de Sandbox (per requeriment tècnic del producte SaaS).
- Associar-li un alias (al SIC 3.0).
- seleccionar l'alias com a proveïdor de seguretat dintre del yaml aca.yml.

3.2.3. Integració KeyCloak

Les SPAs, APPs de mòbil i altres programaris que desitgin consumir una operació publicada a una API amb seguretat OAUTH2 hauran de fer l'inicialització de la llibreria keycloak i fer el SSO/oauth per a obtenir el token bearer que enviaran a la capçalera d'autorització (Authorization) de les seves peticions als gateways.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 15 / 23

3.2.4. El rol “Community Manager/Gestor de comunitat2” és un dels rols estratègics identificats del producte API Connect. Cobreix totes les necessitats d’obtenció d’informació i les capacitats de gestió de les peticions de subscripció de les APPs client.



The screenshot shows the IBM Cloud API Manager interface. The top navigation bar includes 'IBM Cloud', a search bar, and links for 'Catalog', 'Docs', 'Support', 'Manage', and a user profile '1449381 - CENTR'. The main header is 'Privat Preproducció'. Below it, there are tabs for 'Products', 'Consumers', 'Applications', 'Subscriptions', 'Tasks', 'Analytics', 'Members', 'Catalog settings' (selected), and 'Spaces'. A left sidebar lists various management options, with 'Roles' highlighted. The main content area is titled 'Roles' and 'Manage roles and permissions'. It shows a list of roles: 'Viewer', 'Member', and 'Community Manager'. The 'Community Manager' role is expanded, showing a table of permissions for different resources.


Resource	Member	Settings	Topology	Org	Product	Product-Approval
Member	• View	• View	• View	• View	• View	• View
Consumer-Org	• View • Manage	• View • Manage	• Manage	• View • Manage	• View • Manage	• View • Manage
Consumer-Onboard		Api-Analytics	Child			
Approval	• View • Manage	• View • Manage	• View			

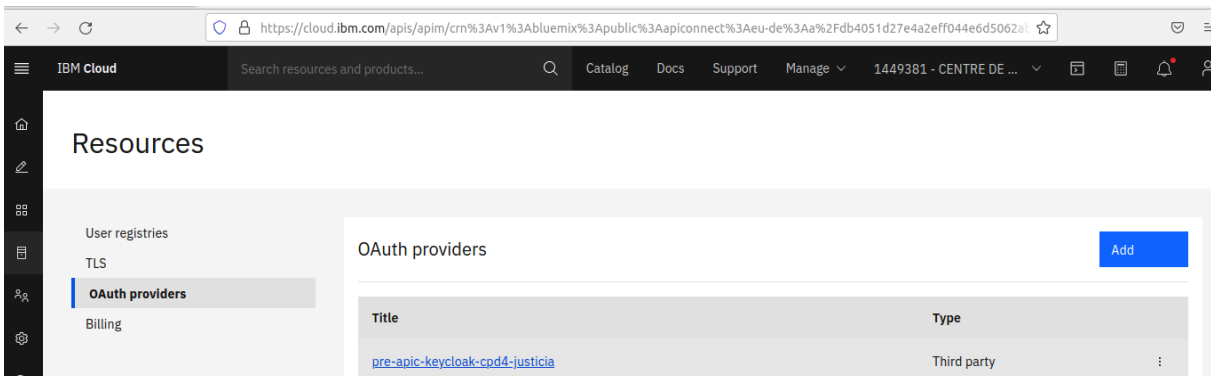
4. Conclusions

Control·lar la forma (plans de consum i requisits d’aprovació) i la seguretat que aplica a les APIs, conjuntament amb la integració de proveïdors oauth2 com ara Gicar/KeyCloak, ens permet tenir el control de quins usuaris efectius consumeixen les APIs publicades en aquesta nova plataforma.

5. Annex

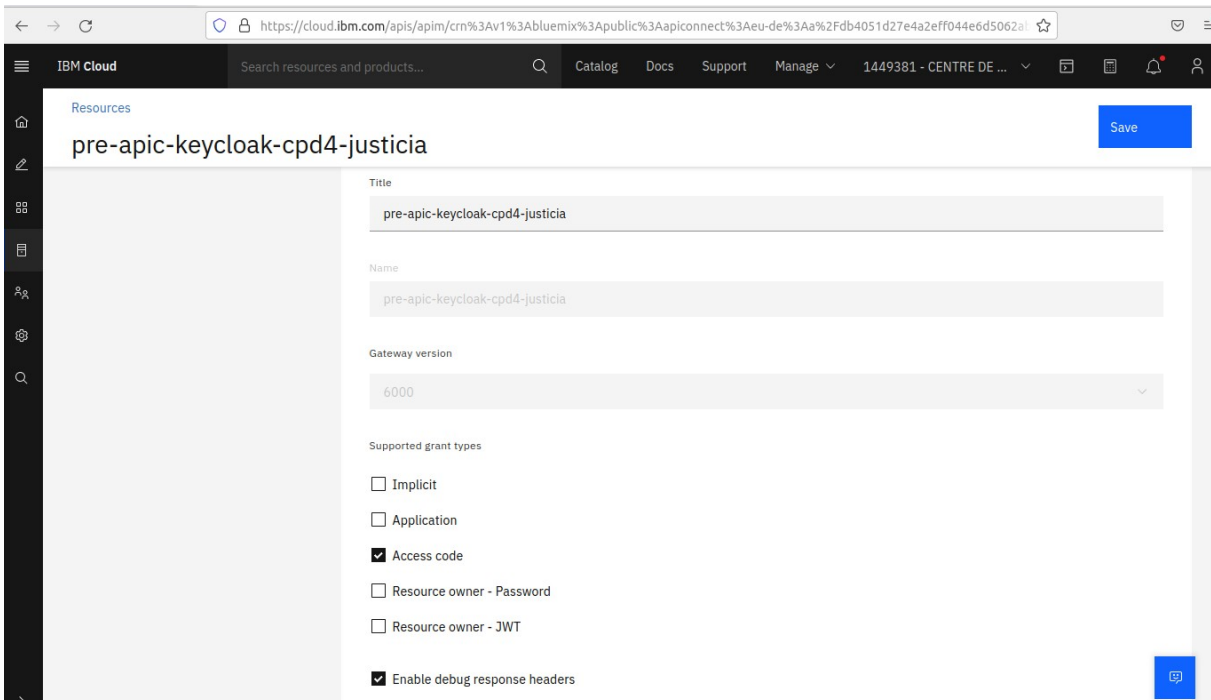
5.1. Configuració KeyCloak

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 16 / 23




The screenshot shows the IBM Cloud API Manager interface. The left sidebar contains a menu with 'OAuth providers' selected. The main content area is titled 'Resources' and displays a table of OAuth providers. One provider is listed with the title 'pre-apic-keycloak-cpd4-justicia' and type 'Third party'. An 'Add' button is visible in the top right corner of the table area.

Title	Type
pre-apic-keycloak-cpd4-justicia	Third party



The screenshot shows the configuration page for the resource 'pre-apic-keycloak-cpd4-justicia'. The page includes a 'Save' button in the top right corner. The configuration details are as follows:

- Title:** pre-apic-keycloak-cpd4-justicia
- Name:** pre-apic-keycloak-cpd4-justicia
- Gateway version:** 6000
- Supported grant types:**
 - Implicit
 - Application
 - Access code
 - Resource owner - Password
 - Resource owner - JWT
- Enable debug response headers

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 17 / 23

Resources

pre-apic-keycloak-cpd4-justicia

Info

Endpoints

Scopes

Endpoints

Define a third-party OAuth provider to issue and validate tokens to protect access to the API.

Authorization URL

`https://preproduccio.keycloak.justicia.intranet.gencat.cat/auth/realms/ejcat/protocol/openid-connect/auth`

Token URL

`https://preproduccio.keycloak.justicia.intranet.gencat.cat/auth/realms/ejcat/protocol/openid-connect/token`

Introspect URL

`https://preproduccio.keycloak.justicia.intranet.gencat.cat/auth/realms/ejcat/protocol/openid-connect/token/introspect`

Introspect cache type

No cache

TLS profile (optional)

`preproduccio.keycloak.justicia.intranet.gencat.cat:1.0.0`

Security (optional)

Resources

pre-apic-keycloak-cpd4-justicia

TLS profile (optional)

`preproduccio.keycloak.justicia.intranet.gencat.cat:1.0.0`

Security (optional)

Basic authentication

Basic authentication request header name (optional)

`x-introspect-basic-authorization-header`

Basic authentication username (optional)

portal


Basic authentication password (optional)

Token validation

Active

Custom header pattern (optional)

Authorization header pass through

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 18 / 23

Resources

pre-apic-keycloak-cpd4-justicia

Info

Endpoints

Scopes

Scopes

Add scopes to allow access to [?](#)

Name	Description
email	email scope
openid	openid scope
profile	profile scope

Advanced scope check after token validation
 Specify the scope check endpoint where additional scope verification is performed in addition to the defined scopes.

Enabled

Activació d'un proveïdor OAUTH2 dins d'un espai (codi de diàleg) i del catàleg de Sandbox (obligatori per requeriment tècnic del SaaS).

Manage / Sandbox /

Sandbox

Products Consumers Applications Subscriptions Tasks Analytics Members **Catalog settings** Spaces

Overview

Gateway services

Lifecycle approvals

Publish validations

Roles

Onboarding

API user registries


OAuth providers

API endpoints

OAuth providers

Manage the OAuth providers configured for API Manager

Title	Type	Description
pre-apic-keycloak-cpd4-justicia	Third party	
apic-keycloak-cpd4	Third party	

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 19 / 23

API Cloud Search resources and products... Catalog Docs Support Manage

Manage / Privat Preproducció / CD1370 /

CD1370

Products Consumers Applications Subscriptions Tasks Analytics Members **Space settings**

- Overview
- Gateway services
- Roles
- Onboarding
- API user registries
- OAuth providers**
- TLS client profiles

OAuth providers

Manage the OAuth providers configured for API Manager

Title	Type	Description
pre-apic-keycloak-cpd4-justicia	Third party	
apic-keycloak-cpd4	Third party	

I un cop tenim activat el proveïdor third-party d'OAUTH2 al CD ja podem publicar APIs que requereixin d'aquest nivell addicional de seguretat.

API Cloud Search resources and products... Catalog Docs Support Manage

Manage / Privat Preproducció /


CD1370

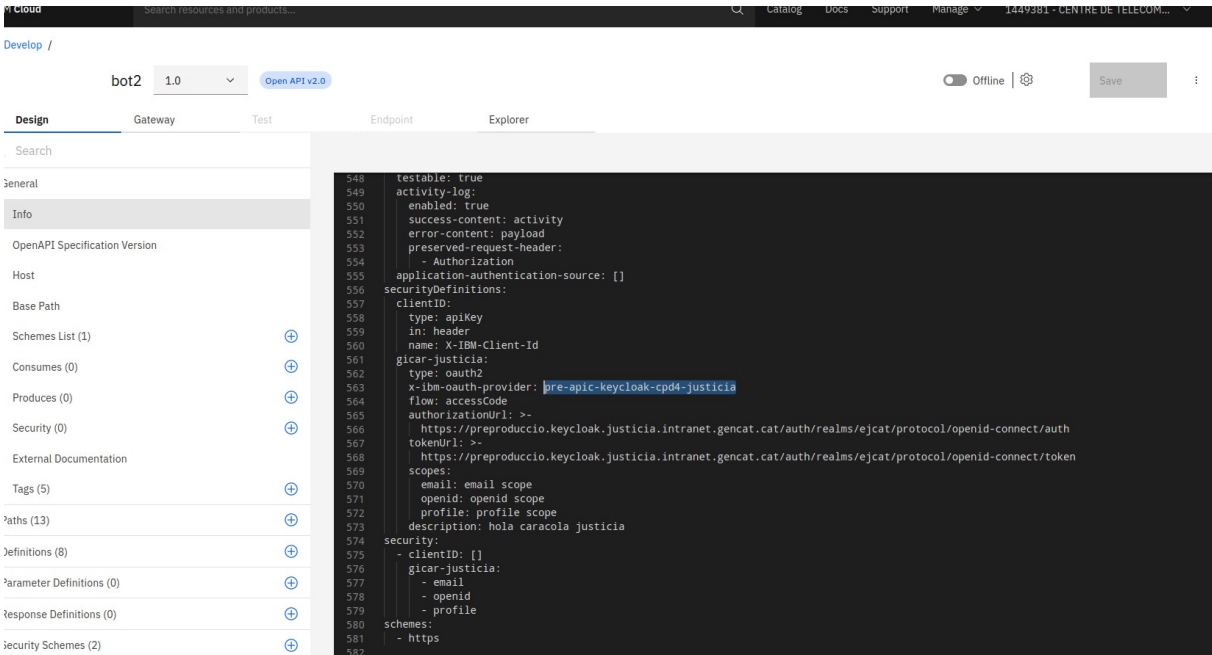
Products Consumers Applications **Subscriptions** Tasks Analytics Members Space settings

Q What are you looking for today?

Product	Product Version	State	Application	Plan	Organization	Modified
bot2	1.0.0	enabled	bot app	Default Plan	joan joan	fa 7 hores
cat-fact-product	1.0.0	enabled	DEMO V	Default Plan	Opentrends	fa un dia
cat-fact-product	1.0.0	enabled	Demo	Default Plan	Organization II	fa 15 dies
demo-paco-prod-pre	1.0.0	enabled	Demo	Default Plan	Opentrends	fa un mes

bot2 és l'exemple d'un producte publicat (amb subscripcions actives) que inclou una API que requereix l'autenticació amb el KeyCloak de Justicia.

	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 20 / 23



```

548 testable: true
549 activity-log:
550   enabled: true
551   success-content: activity
552   error-content: payload
553   preserved-request-header:
554     - Authorization
555   application-authentication-source: []
556 securityDefinitions:
557   clientId:
558     type: apiKey
559     in: header
560     name: X-IBM-Client-Id
561   gicar-justicia:
562     type: oauth2
563     x-ibm-oauth-provider: pre-apic-keycloak-cpd4-justicia
564     flow: accessCode
565     authorizationUrl: >-
566       https://preproduccio.keycloak.justicia.intranet.gencat.cat/auth/realms/ejcat/protocol/openid-connect/auth
567     tokenUrl: >-
568       https://preproduccio.keycloak.justicia.intranet.gencat.cat/auth/realms/ejcat/protocol/openid-connect/token
569     scopes:
570       email: email scope
571       openid: openid scope
572       profile: profile scope
573     description: hola caracola justicia
574   security:
575     - clientId: []
576     - gicar-justicia:
577       - email
578       - openid
579       - profile
580   schemes:
581     - https
582

```

L'api bot2 publicada amb 2 requeriments de seguretat:

1. IBM client-id és el requeriment estàndard de seguretat mínim acceptable (implica subscripció i aprovació de subscripció al producte).
2. Autorització validada mitjançant el proveïdor de seguretat que està disponible dins l'espai on es publica el producte/API.

5.2. Configuració KeyCloak al codi client

Exemple d'ús del keycloak javascript adapter:

Cap problema, et passo el codi del HTML (en groc el que s'ha de posar per inicialitzar el Keycloak Javascript Adapter):


```

<html>
  <head>
    <script src="dist/keycloak.js" type="text/javascript">
    </script>
  </head>

  <body>
    <h1>Aplicació de proves Keycloak GICAR</h1>

    <div>
      L'usuari <b id="subject"></b> ha fet aquesta petició.
    </div>
  </body>
</html>

```

	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 21 / 23


```

<p><b>Detalls de l'usuari (extrets de <span id="profileType"></span>):</b></p>
<p>Nom d'usuari (NIF): <span id="username"></span></p>
<p>Email: <span id="email"></span></p>
<p>Nom complet: <span id="name"></span></p>
<p>Nom: <span id="givenName"></span></p>
<p>Cognoms: <span id="familyName"></span></p>
<p><b>-----</b></p>
<p><b>Altres dades:</b></p>
<p>Access Token: <span id="tokenbearer"></span></p>
<p>Resposta User Info (extreta de resposta a l'API): <span
id="respostaUserInfo"></span></p>
<p>Resposta api manager (extreta de resposta a l'API): <span
id="respostaApiManager"></span></p>

</div>

<script type="text/javascript">
var keycloak = Keycloak("http://localhost:3000/keycloak.json");
var loadData = function () {
document.getElementById('subject').innerHTML = keycloak.subject;
if (keycloak.idToken) {
document.getElementById('profileType').innerHTML = 'IDToken';
document.getElementById('username').innerHTML =
keycloak.idTokenParsed.preferred_username;
document.getElementById('email').innerHTML = keycloak.idTokenParsed.email;
document.getElementById('name').innerHTML = keycloak.idTokenParsed.name;
document.getElementById('givenName').innerHTML =
keycloak.idTokenParsed.given_name;
document.getElementById('familyName').innerHTML =
keycloak.idTokenParsed.family_name;
document.getElementById('tokenbearer').innerHTML =
keycloak.token;
} else {
keycloak.loadUserProfile(function() {
document.getElementById('profileType').innerHTML = 'Account Service';
document.getElementById('username').innerHTML =
keycloak.profile.username;
document.getElementById('email').innerHTML = keycloak.profile.email;
document.getElementById('name').innerHTML = keycloak.profile.firstName
+ ' ' + keycloak.profile.lastName;
document.getElementById('givenName').innerHTML =
keycloak.profile.firstName;
document.getElementById('familyName').innerHTML =
keycloak.profile.lastName;
document.getElementById('tokenbearer').innerHTML = keycloak.token;
}, function() {
document.getElementById('profileType').innerHTML = 'Failed to retrieve
user details. Please enable claims or account role';

```

	API Manager - Manual de seguretat	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 22 / 23


```

});
}

var url = 'https://preproduccio.endpointma.autenticaciogicar4.extranet.gencat.cat/realms/gicarcpd4/protocol/openid-connect/userinfo';
var req = new XMLHttpRequest();
req.open('GET', url, true);
//req.setRequestHeader('Accept', 'application/json');
req.setRequestHeader('Accept', 'application/x-www-form-urlencoded');
req.setRequestHeader('Authorization', 'Bearer ' + keycloak.token);
req.onreadystatechange = function () {
if (req.readyState == 4) {
if (req.status == 200) {
//var users = JSON.parse(req.responseText);
//var html = "";
//for (var i = 0; i < users.length; i++) {
//    html += '<p>' + users[i] + '</p>';
//}
document.getElementById('respostaUserInfo').innerHTML =
req.responseText;
//document.write(req.responseText);
console.log('finished loading data');
}
}
}
req.send();

//var url2 =
'https://preproduccio.ctti.apim.intranet.gencat.cat/ctti/privat-pre/api/v1/actuator/health';
//var url2 =
'http://limsunsangnim.efile.kr:8080/~weedscut/javascript/AjaxInAction/ch11/server_src/content/headers.jsp';
//var url2 =
'http://preproduccio.bot.ejcat.justicia.intranet.gencat.cat/api/v1/actuator/health';
//var url2 = 'https://catfact.ninja/fact';
var url2 =
'https://preproduccio.ctti.apim.intranet.gencat.cat/ctti/privat-pre/cat-fact/';
var req2 = new XMLHttpRequest();
req2.open('GET', url2, true);
//req2.setRequestHeader('Accept', 'application/json');
req2.setRequestHeader('Accept', 'application/x-www-form-urlencoded');
req2.setRequestHeader('Authorization', 'Bearer ' + keycloak.token);
req2.setRequestHeader('x-ibm-client-id',
'c8c2c4409c0e6b56e6a6262c8d69a215');
//req2.setRequestHeader('Origin', 'http://localhost:3000/index2.html!');

```

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	<i>API Manager - Manual de seguretat</i>	N. revisió doc.: 1.0
	Manual d'usuari	
	N. versió solució: 1.0	Pàg. 23 / 23

```

req2.onreadystatechange = function () {
  if (req2.readyState == 4) {
    if (req2.status == 200) {
      //var users = JSON.parse(req.responseText);
      //var html = "";
      //for (var i = 0; i < users.length; i++) {
      //    html += '<p>' + users[i] + '</p>';
      //}
      document.getElementById('respostaApiManager').innerHTML =
req2.responseText;
      //document.write(req.responseText);
      console.log('finished loading data api manager');
    }
  }
  req2.send();
};

var loadFailure = function () {
  document.getElementById('customers').innerHTML = '<b>Failed to load data.
Check console log</b>';
};

var reloadData = function () {
  keycloak.updateToken(10)
    .success(loadData)
    .error(function() {
      document.getElementById('customers').innerHTML = '<b>Failed to load
data. User is logged out.</b>';
    });
}

keycloak.init({ onLoad: 'login-required' }).success(reloadData);
</script>

<br><br>
<button onclick="reloadData()">Reload data</button>
</body>
</html>

```

Podeu trobar més informació al respecte els clients existents a: <https://www.keycloak.org/>