O DAMER 2.0. L' MUN protocolo de de legação, permitindo a MUN dono dum recurso autorizar MUNA aplicação para aceder ao recurso, seu que esta possa fazer passar-se pelo dono do recurso.

Entidaden:

- Resonnce Owhen (Ro) - Tem acesso a

MULL API e pode delegan acesso a essa

API. D resonnce owhen e' usualulute

API. D resonnce owhen e' usualulute

MULL PESSOC e e' ghalulute assumido que

MULL HUM Growsen.

Componente sobre o qual o Ro tem acesso. É geralmente assumido que o PR e mua Web API.

L'openagoes len, encrever, ...

- Client Peça de software que acede ao PR em lugar do RO.
- Anthonization Server (A5) Entidade confiavel
 pelo PR que quite enedeuciais de segurança,
 chamadas OAuth Access tokens (AT), aos
 chientes.

Para adquirir mu AT, o cliente envic o Ro ao AS para que o Ro autorize o Cliente junto do AS. O RO autentice-se no AS e 3. autorize o chilute pare aceder a mu coajmuto de scopes (suscoujmuto de funcionalidades).

Assim que o As autorize o cliente, o cliente, o cliente pode solicitar um Access Token (AT) ao AS.

O AT l'apresentado ao PR pelo cliente para aceder à sua API, como delegado pelo RO.

As inedenciais de Ro muca são expostas ao cliente.

EX: RO-Dono de fotognatian

Client - Senviço Web de impressas

de fotografian

PR- Senvidor oude então an

fotografias

Protected Anthonization RLDOUNCE Clifat Resource serul Chilute pede autorização Owher no da antonização cliente envie autorização concedida AS envia access token chilute envie access token PR envia necurso

Nota: O AS Tem que conhecen

o cliente para que possau interagir.

Assim, o cliente Tem que se registar

junto do AS.

P. ex., através dum

"developer pontal"

Após o registo, o As atribui mu client-id e mu client-secret (no caso de se tratar dum confidential client).

	0 177 000	De C = 10	11 10 1	~6 (AMCO		Ю -
RESOMACE	CL	teat		ithorizat			Protected Resource
) when	nedineci	bи а	1 Author	rigation point	TOK.	en Ipoiut	
6 www se	n p/ A5	Auth.					
end p	pojnt 						
brow.	su carrl	ja ende	oint.				
K	20 auto	itica-se	NO AS	e aut	oniza	cliente	
<	re direción	16 61011	500 0/	e lila te			
A) Com	reamecros authoriza	tion (00	le -	->0.12 (0 -			
Ŀ							
5 now ser	n carrescou	redirect	t ORI				
do ch		. 0-04	T. 0/1	ria anth	. code +	credencia.	κis
		clilu	te do	token e	eud point		
		AS e	uvia	accenn t	to Ken	ro clien	Ū
					20 / 1		PP
		clieul	e en	ric acc.	epp to	Kln ao	
		10.0	0 (0 V)	a recu	MO a	o clien-	te
		PR	Ž.K.				

NO DANTH Dão MARdon Blaner tokeus (tokeus de Portadon)

Lo vantagem: chiente não precisa de des codificar/processar os Bearen tokens (são opacos) e, mma vez na sua posse, pode msá-los sem restrições (funciona como mma password).

Lo existen on two tokens, ex: JWT (JSON Web TOKENS), pop (Proof of Possession),...

Refresh tokens (RT) - Semethante a mm acceps token, mas um refresh token mhac e' enviado ao Protected Resonnace.

O chilule envir nou RT ao AS para solicitar novo access token sem envolver o Resource Owner (este pode até ja' nas se encontrar online).

Authorization Server

Pede recurso com accepo token

ERRO! TOKER invalido/expinado

Envic refresh token

Retorna novos access token e refresh token ao cliente

pede recurso com novo access token

OK, devolve recurso

Scopen - Mecanismo unado para limitar acesso do chiquée aos recursos.

co definido pelo Protected Resonnes us representado por conjunto de strings ex: read-photo, read-metadata,...

9.

OU URI

Interação entre atores e componentes; back channel e front channel

Back channel - Pedidos e respostas HTTP entre componentes banth (usando hecders, query paremeters, methods, body) que não envolvem o user agent (Growser) nem o

RESOUNCE DWHER.

Client Elient Server

Protected Resonace

Front-channel - Comunicação

front-channel e' nun método de uran pedidor HTTP para comunicar indiretamente entre doir sistemas por intermédio dum browser.

ex: Resonnce Owner autentica-se no AS
seu mostrar as creadenciais ao cliente.

Resource HTTP

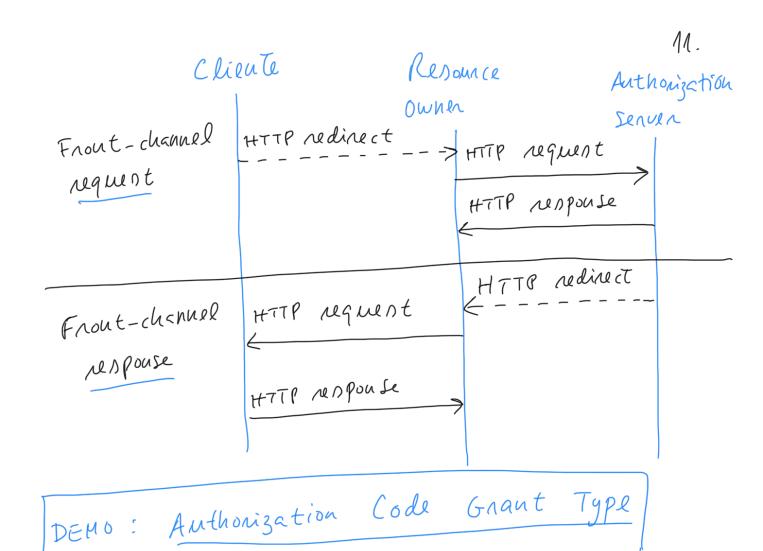
OWHER

FITTP

HTTP

Redirects

Chilat



Gexistem outros fluxos, como:

- implicit grant type

- client credentials grant type

- · Formas de enviar um Blaner token:
 - -HTTP Anthonization headen (preferencial)
 - form-encoded request body parameter

 Univa POST + forms
 - URL-Rucoded query parameter

 URL-Rucoded query parameter

 URL-Rucoded query parameter

 Saccesso token pode ser capturado

 pois vai no URL request