Protocols d'autenticació i autorització en aplicacions i serveis web

Pau Gibert, Mireia Grueso, Abel Gallardo, Victoria Puszyn

Definicions

AUTENTICACIÓ:

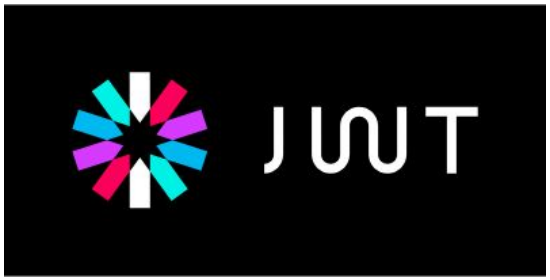
Conjunt de regles i procediments que s'usen per a verificar la identitat d'un usuari o entitat que intenta accedir a un sistema o una xarxa

AUTORITZACIÓ:

Procés que s'usa per a decidir si la persona, programa o dispositiu té permís per a accedir als recursos del sistema

IMPORTÀNCIA: S'usen per a proporcionar un mecanisme o procediments per a verificar la identitat de les entitats que es comuniquen i protegir-se contra el accés no autoritzat o la manipulació

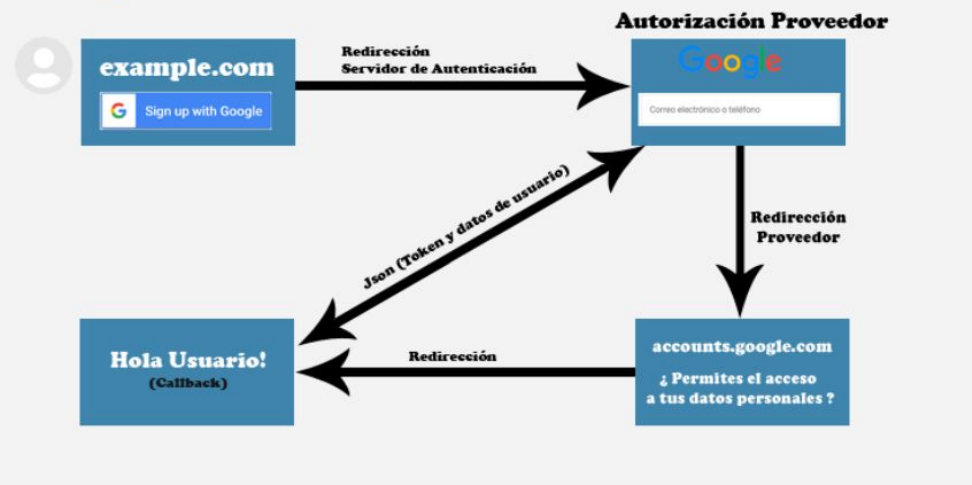
Exemples



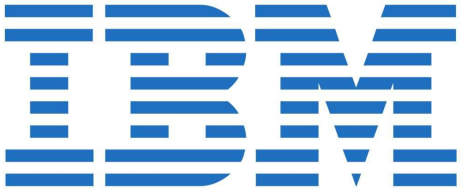
PROTOCOL D'AUTENTICACIÓ: OpenID

Descripció

- Protocol de **autenticació de identitat**.
- Permet l'autenticació en serveis externs compatibles amb OpenID mitjançant una **URL**.
- Basat en **OAuth 2.0** (OpenID Connect).



Exemples de proveïdors d'identitats OpenID



Versions

OpenID 1.0 (2005):

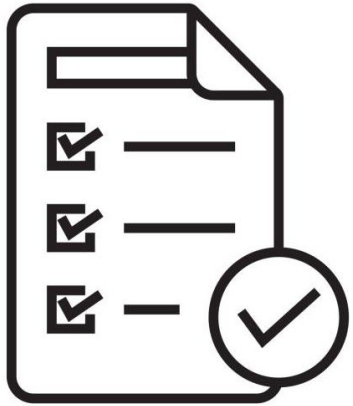
- Autenticació d'usuaris.
- Limitacions i problemes de seguretat.

OpenID 2.0 (2006):

- Soluciona problemes 1.0
- Inclou l'ús d'extensions
- Va ser ampliament utilitzada en el seu temps.

OpenID Connect 1.0 (2014):

- Usa OAuth 2.0 com a base.
- Proporciona autenticació i autorització en un sol flux.
- Introducció dels Tokens de identificació.
- Actualment està molt extesa aquesta versió del protocol.



Avantatges i desavantatges

AVANTATGES

- **Autenticació de l'usuari simplificada.**
- **Major interoperabilitat.**
- **Experiència d'usuari millorada.**

DESAVANTATGES

- Vulnerabilitat de seguretat.
- Dependència cap als proveïdors d'identitat.
- Implementació complexa.

PROTOCOL D'AUTENTICACIÓ: SAML

Descripció

Codi obert en XML

SAML v2.0

Intercanviar informació d'autenticació i autorització

Solució completa per a la gestió de la identitat federada (FIM)

Exemples d'aplicacions i serveis que usen SAML

Versions


SAML 1.0
SAML 1.1
SAML 2.0
Març de 2001
Febrer de 2003
Març de 2005
Introducció del model SAML
Millora compatibilitat
SSO
Federació d'identitat
Introducció de metadades

Avantatges i desavantatges

AVANTATGES

- Autenticació única (SSO)
- Centralització de l'autenticació
- Seguretat millorada
- Flexibilitat i interoperabilitat

DESAVANTATGES

- Dependència d'internet
- Limitacions en disp. mòbils
- Costos inicials

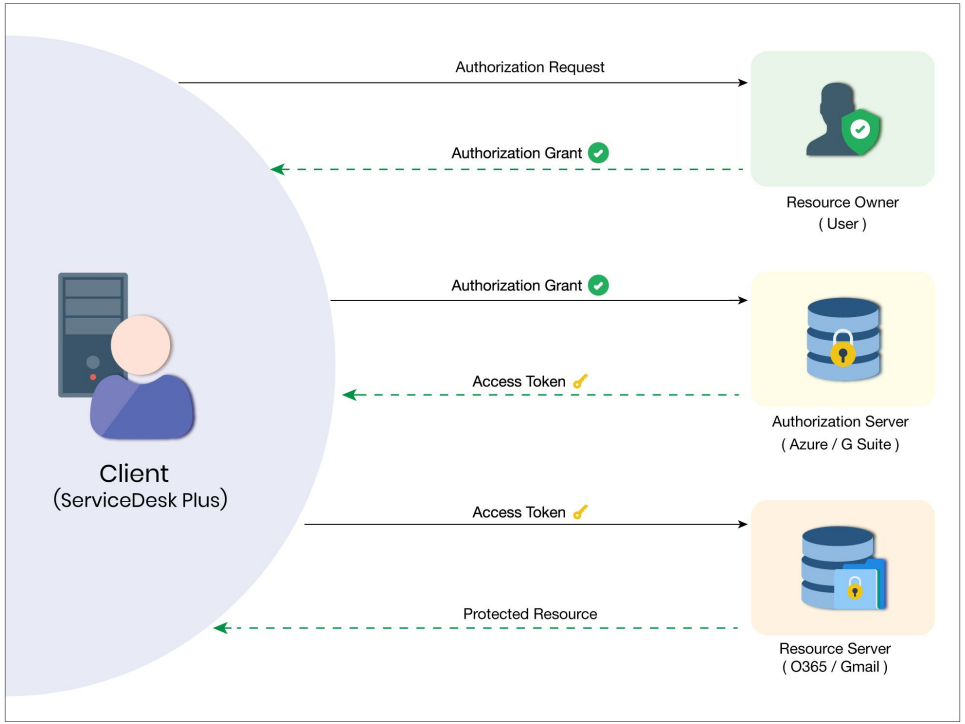
PROTOCOL D'AUTORITZACIÓ: OAuth

Descripció

OAuth = Open Authorization

- Protocol estàndard d'autorització
- Utilització de "tokens" d'accés

Ús de rols i permisos



Millores del OAuth 2.0

Eliminació de Signatures Criptogràfiques: simplificació comunicacions màquina a màquina

Bearer Tokens per a Simplicitat: simplificació de l'autorització, no requereix signatura complicada

Terminologia Renovada i Més Clara: de Consumidor a Client i de Proveedor de Serveis a Servei d'Autorització

Tokens d'Actualització per a Manteniment Continu: permet renovació de permisos sense nova interacció de l'usuari

Exemples pràctics del funcionament en aplicacions web

1. Iniciar Sessió i Configuració a Pinterest
2. Habilitar Connexió amb Facebook
3. Aprovació de Autorització
4. Sol·licitud d'Access Token
5. Accés als Dades Protegits
6. Importació a Pinterest

Avantatges i desavantatges

AVANTATGES

- OAuth 1.0
  - Seguretat no completament delegada a HTTPS/TLS
  - Basada en criptografía

- OAuth 2.0
  - Delega moltes defenses a HTTPS/TLS
  - Integració més senzilla amb “Bearer Tokens”
  - Més fàcil de treballar
  - Més flexible
  - Millor separació de tasques

DESAVANTATGES

- OAuth 1.0
  - Més complexitat
  - Gestió cuidadosa
  - Menys flexibilitat

- OAuth 2.0
  - Vulnerabilitat
  - Relativa facilitat per ser copiats/robats
  - Complexitat addicional
  - Requereix validació precisa

Conclusions

Referències utilitzades:

Què és l'autenticació?

Autorització i control d'accés

OAuth | Todas las claves del protocolo y de su versión OAuth2 - IONOS

What's the Difference Between OAuth 2.0 and OAuth 1.0? | Synopsys Blog

Com funciona OpenID

OpenID descentralitzant la teva identitat online

Introducció a OpenID

Repartiment tasques

- **Pau Gibert**: Presentació + Definicions i Conclusions
- **Mireia Grueso**: OpenID - Descripció, exemples de proveïdors d'identitats, versions, avantatges i desavantatges
- **Abel Gallardo**: SAML - Descripció, exemples d'aplicacions i serveis que s'utilitzen, versions, avantatges i desavantatges
- **Victoria Puszyn**: OAuth - Descripció, ús de rols i permisos, millores d'OAuth 2.0, exemples pràctics, avantatges i desavantatges