# Xestión de Identidades

Os Servicios de Directorio

# A Xestión de Identidades

A ***xestión de indentidades*** se encarga de controlar a identificación das entidades (usuarios e sistemas) que acceden aos distintos recursos. Este proceso debe establecer qué sistemas son accesibles para cada entidade e que nivel de privilexios pode ter sobre eles.

A xestión de identidades é imprescindible hoxe en día xa que as compañías teñen unha gran cantidade de usuarios de IT e un gran conxunto de elementos sobre os que se deben controlar os privilexios.

Un sistema de xestión de identidades:

- **Identifica** e **autentica** as entidades
- **Autoriza** o seu acceso
- Xestiona as contas e a súa información asociada (credenciais, atributos...)
- Permite un acceso único a todos os recursos da rede (Single Sign On)
- Xestiona os privilexios a nivel individual e por grupos
- Xestiona o ciclo de vida dos usuarios (creación, mantemento, borrado)
- Audita e monitoriza o uso das contas e os accesos

# Autenticación, Identificación e Directorio

Se coñece como ***Single Sign On*** (SSO) o procedementode identificación e autenticación que permite a un usuario autenticarse unha única vez para acceder a diferentes recursos sin ter que volver a facilitar as súas credenciais. Isto ofrece varias ventaxas:

Dende o punto de vista do usuario:

- Non precisa introducir varias veces as súas credenciais
- Non precisa memorizar varias credenciais

Dende o punto de vista dos administradores:

- Permite unificar a xestión das contas e privilexios de acceso de diferentes aplicacións

Dende o punto de vista de seguridade:

- Reduce o risco de roubo de credenciais
- Facilita a xestión de credenciais. Unha baixa de credenciais impedirá o acceso a todos os recursos, unha alta o permitirá.
- Unifica a política de robustez de contrasinais en todas as aplicacións.

Unha parte moi importante da xestión de identidades é a Identificación e Autenticación. Esta identificación idealmente debe ser centralizada: As entidades se deberían identificar e autenticar nun servidor de autenticación que valide a identidade para toda a rede de xeito que as credenciais se suministren o mínimo número de veces. A outra parte é a recuperación da información relevante dos usuarios, para o que se utilizan os ***Servizos de Directorio***

# Servizos de Directorio

Un Directorio é unha base de datos optimizada para lectura e busca de información que almacena información sobre os recursos dunha rede e dos seus usuarios. O formato de directorio máis extendido sigue o estándar **X.500**, baseado nunha estrutura xerárquica.

No directorio se almacena información como atributos dos usuarios, perfís de autorización, roles, políticas de control de acceso…..

O protocolo de acceso a servizos de directorio máis coñecido é LDAP (Lightweight Directory Access Protocol).

***Microsoft Active Directory*** é a solución de directorio máis estendida. Básicamente consiste nunhha base de datos de directorio LDAP que utiliza un servizo *Kerberos* para a autenticación e autorización.

Outros servizos de directorio coñecidos son:

***OpenLDAP:*** Base de datos de directorio baseada no protocolo LDAP.

***SAMBA:*** Utiliza LDAP+Kerberos para proporcionar servizos de directorio compatibles con Microsoft Active Directory

***Novell e-Directory:*** Solución de Novell similar a Active Directory

***Oracle Directory Server Enterprise Edition****:* Solución de Oracle baseada en LDAP tamén similar a Active Directory

Os servizos de directorio deben empregar sistemas de autorización e identificación, sendo o máis común **Kerberos**

# Servicios de Autenticación e Identificación
## Kerberos

***Kerberos*** é un protocolo de identificación e autenticación que utiliza cifrado simétrico para autenticar entidades contra servizos de rede **sin necesidade do envío de contrasinais** a través da rede, evitanto ataques de intercepción de contrasinais.

Esta tarefa a leva a cabo mediante un servidor (terceiro de confianza) que se encarga de autenticar un cliente para un servizo (e o servizo para o cliente) denominado KDC (Key Distribution Center). O KDC emprega dous compoñentes asociados, o servizo de autenticación AS (Authentication Server) e o servidor de tickets TGS (Ticket Granting Server).

Cada entidade ten unha chave segreda que únicamente coñecen Kerberos e a entidade. Cando desexa acceder a un servizo, Kerberos xenera unha chave de sesión (ticket) que se utilizará para o acceso seguro. O proceso é o seguinte:

1) Cando unha entidade quere utilizar un servizo de rede (NS) o solicita ao KDC.
2) O KDC pasa a petición ao AS que crea un ticket (TGT) que leva unha chave de sesión cifrada coa chave do usuario.
3) O usuario descifra o ticket coa súa chave, e a devolve ao KDC cifrada indicando a qué recurso quere acceder.
4) O TGS crea un ticket con dúas mensaxes. Unha cifrada coa chave do usuario incluíndo a chave para a sesión co recurso, e outra cifrada coa chave do recurso ao que se desexa acceder (NS). Os dous tickets levan información sobre o usuario, a chave de sesión co recurso e unha marca de tempo.
5) O usuario descifra a mensaxe  cifrada coa súa chave obtendo a chave de sesión, e envía ao servidor (NS) un ticket coa información da súa mensaxe cifrada coa chave de sesión e a mensaxe de acceso o recurso, que estaba cifrada coa chave do servidor (NS)
6) O servidor (NS) descifra o seu ticket e obten a chave de sesión. Con ella pode descifrar a outra mensaxe, e si o consigue, acepta suministrar o servizo.

Como vemos, na comunicación se identifica e autentica tanto o cliente (si o cliente non é lexítimo non será capaz de descifrar a parte apropidada do primeiro ticket) como o servidor (si o servidor non é o lexítimo, non será capaz de descifrar o ticket que envía o usuario)

# Servicios de Autenticación e Identificación

## SAML (Security Assertion Markup Language)

SAML é un estándar para o intercambio de información de autenticación e autorización entre dominios baseado en XML. A versión que se utiliza na actualidade é SAML 2.0 e se emprega para implementar servizos de autenticación SSO (Single Sign On). O procedemento é o seguinte:

1) O usuario (por exemplo un navegador) intenta acceder a un recurso (proveedor de servizos)
2) O proveedor de servizos determina qué proveedor de identidade utilizar e redirixe hacia él ao usuario incluíndo na resposta a identificación do servizo
3) O usuario solicita autenticación ao proveedor de identidade, que devolve un documento XHTML coa información de autenticación que precisa o servizo. O usuario reenvía ese documento ao proveedor de servizos. Si o usuario non facilita ningún token de sesión, solicitará previamente as credenciais.
4) O proveedor de servizos procesa a resposta e crea un contexto de seguridade ( rexistro ) e facilita o acceso ao servizo.

# Servicios de Autenticación e Identificación
## OAuth

Oauth é un estandar para **autorización**, non autentica, sendo necesario recurrir a un servicio de autenticación como OpenID. O seu obxectivo é autorizar a dous servicios dun usuario a interactuar entre eles. Vexamos un exemplo:

**Actores:**

- Usuario (Resource owner), é o dono dos dous servizos.
- Servizo cliente A (Client) é o servizo que quere utilizar o servizo proveedor (por exemplo, Spotify)
- Servizo proveedor B (Resource server) é o proveedor do servizo que quere ser utilizado por A (por exemplo, Facebook)
- Servizo de autorización (Authorization Server), que é o xestor das autorizacións, por exemplo Facebook.

**Funcionamento:**

- Spotify pide permiso ao Usuario para poder postear en Facebook
- O usuario lle concede permiso
- Spotify envía a Facebook (Authorization Server) o OK do usuario
- Facebook (Authorization Server) devolve a Spotify un token de acceso
- Spotify usa ese token para poder postear en Facebook (Resource Server) mentres non caduque o token

# Servicios de Autenticación e Identificación
## OpenID

OpenID é un proceso de autenticación pensado para funcionar con OAuth. O seu obxectivo non é a autorización de acceso, se non a autenticación dun recurso.

- O sitio web “sitio.com” desexa ofrecer acceso aos visitantes mediante OpenID, para o que facilita un formulario de acceso pedindo únicamente o identificador OpenID.
- O usuario “María” quere acceder a “sitio.com”, para o que utiliza o seu identificador OpenID “maria.proveedor-openid.org”, rexistrada no proveedor de identidade proveedor-openid.org
- O sitio web “sitio.com” contacta con proveedor-openid.org. Pode facelo directamente sin intervención do usuario (checkid_inmediate) ou poñendo en contacto ao usuario co proveedor de identidade (checkid_setup).
- “sitio.com” almacena unha chave compartida co proveedor de identidade (proveedor-openid.org), si se emplea checkid_setup, se redirixe a maria a páxina de proveedor-openid.com para que se autentique, si xa ten unha sesión aberta, únicamente preguntará sobre a confianza que otorga a “sitio.com” para acceder aos seus datos. Tras a autenticación “María” é redirixida a “sitio.com” coas credenciais de autenticación obtidas que se verificarán coa chave compartida.
- “sitio.com” considera a “María” como rexistrada co seu ID OpenID, e si é necesario solicita información adicional para rematar o rexistro.

# Servicios de Autenticación e Identificación

## Acceso Remoto AAA (Authorization, Authentication and Accounting) - RADIUS

***RADIUS (Remote Authentication Dial In User Service)*** é un protocolo de rede que proporciona autenticación, autorización e auditoría para conexións remotas. As credenciais do usuario se envían a un servidor de acceso (AS). Este servidor de acceso, enviará as credenciais ao servidor RADIUS que as validará.

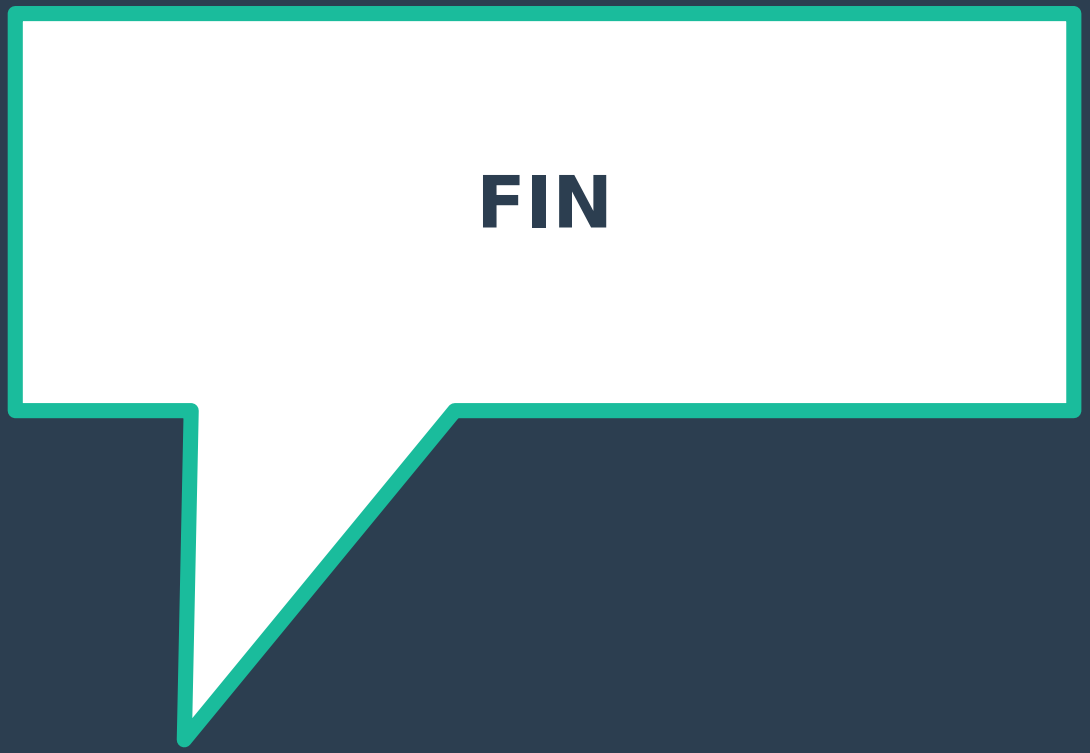
RADIUS utiliza o protocolo UDP e únicamente cifra o contrasinal entre o cliente e o servidor de autenticación.

RADIUS é o estándar para a conexión segura a redes WiFi mediante WPA2-Enterprise.

# Servicios de Autenticación e Identificación

## Acceso Remoto AAA (Authorization, Authentication and Accounting) - TACACS

**TACACS (Terminal Access Controller Access Control System)** é similar a RADIUS e se utiliza para a xestión remota de elementos de rede (switches, routers...). Está baseada en TCP e cifra toda a información que se transmite, polo que se considera máis segura que RADIUS.


FIN