Texto Intro ABAC

ABAC (attribute-based access control)

A diferencia de RBAC, en un sistema de control de acceso basado en atributos (**ABAC**), cualquier tipo de atributo —como los atributos de usuario y los atributos de recursos— se utilizan para determinar el acceso.

En **ABAC, un atributo** es una característica que se utiliza para definir las políticas de acceso y tomar decisiones de acceso a recursos protegidos. Un atributo puede ser cualquier tipo de información que sea relevante para la política de acceso, como la identidad del usuario, su ubicación, su función dentro de la organización, la hora del día, entre otros.

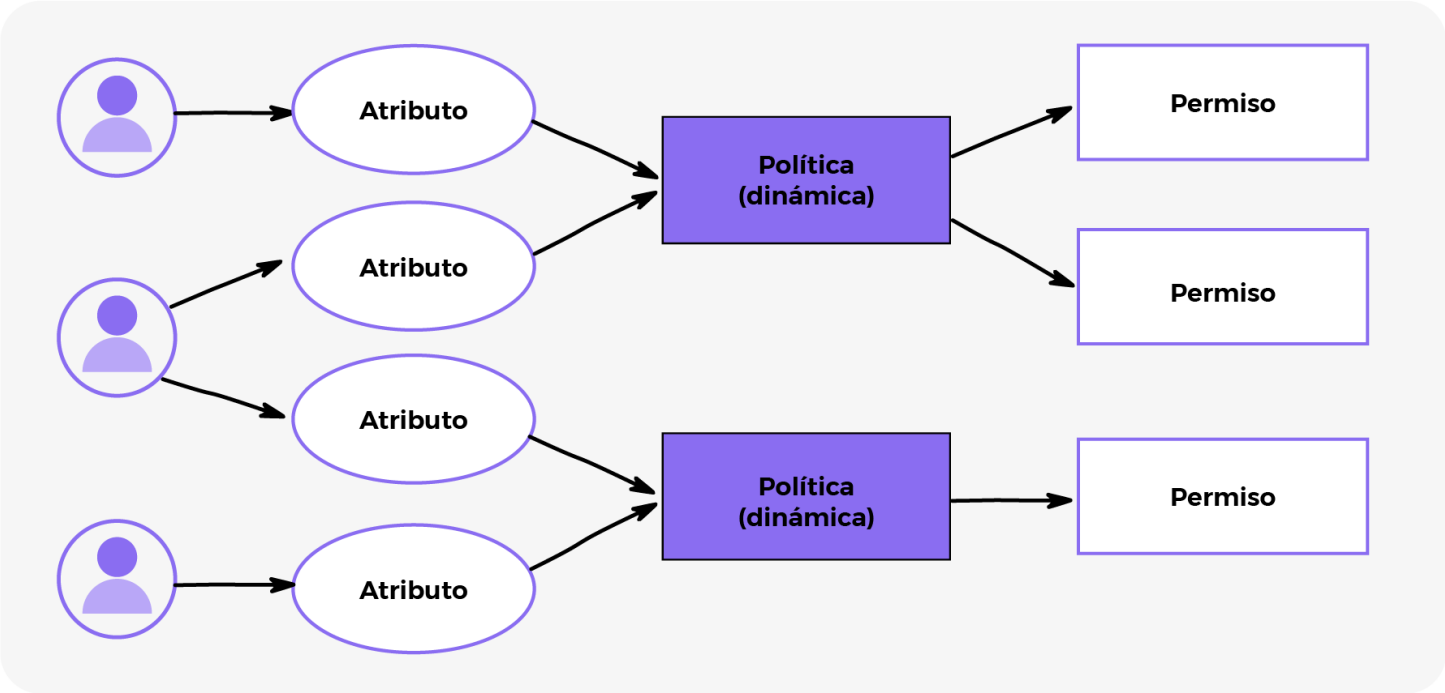
Un **ejemplo de un atributo en ABAC** sería por ejemplo la afiliación/pertenencia de un usuario. En este caso, el atributo podría tomar el valor de "miembro" o "no miembro" de una determinada organización o grupo. La política de acceso podría establecer que solo los usuarios que sean miembros de una organización específica tengan acceso a ciertos recursos protegidos.

Otro ejemplo de atributo podría ser la ubicación geográfica del usuario. En este caso, el atributo podría tomar valores como "dentro de la red de la empresa" o "fuera de la red de la empresa".

Estos atributos se comparan con valores estáticos definidos o incluso con otros atributos, lo que lo convierte en un control de acceso basado en relaciones.

Los atributos vienen en pares clave-valor (como por ejemplo "Rol = Supervisor"), que se pueden usar para limitar el acceso a una determinada característica de un sistema. Es decir, que este tipo de control utiliza los atributos que contiene el token e información sobre el contexto de autorización para conceder acceso a los recursos.

ABAC se considera una forma más flexible y granular de control de acceso que otros modelos, como el control de acceso basado en roles (RBAC) o el control de acceso basado en permisos (PBAC), ya que permite la creación de políticas de acceso más detalladas y sofisticadas.



Los **tokens** se utilizan para tomar decisiones de acceso en **ABAC**. Cuando un usuario solicita acceso a un recurso protegido, el sistema de control de acceso utiliza los **claims** contenidos en el **token** del usuario para determinar si tiene los permisos necesarios para acceder al recurso.

¿Qué es un CLAIM?

Un **claim** es un dato en particular que se utiliza para describir un usuario o una entidad y que se utiliza para tomar decisiones de acceso.

Los **claims** pueden ser cualquier tipo de información que sea relevante para la política de acceso, como el nombre del usuario, su correo electrónico, su identidad federada, su cargo dentro de la organización, entre otros.

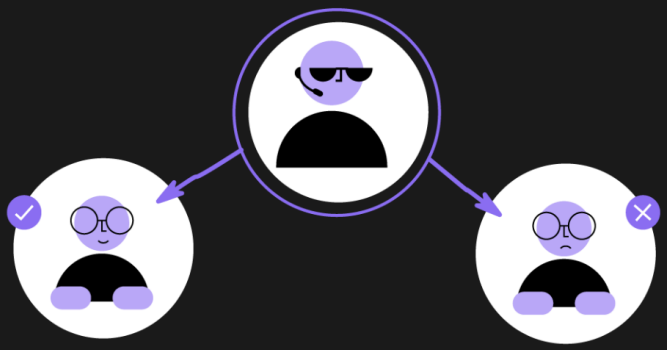
Un claim suele estar formado por dos partes: el nombre del claim y el valor del claim. El nombre del claim es una cadena de caracteres que describe el tipo de información que se está proporcionando, como "nombre", "correo electrónico" o "cargo". El valor del claim es el valor real de la información proporcionada, como "Juan Pérez", "juan.perez@empresa.com" o "Gerente de Recursos Humanos".

Por ejemplo, un claim podría ser "cargo: Gerente de Ventas". Si un recurso protegido requiere que los usuarios tengan el rol de gerente de ventas para acceder, entonces la política de acceso ABAC se puede configurar para que solo los usuarios que tengan ese claim específico puedan acceder al recurso.

Roles dentro de KEYCLOAK

Para poder utilizarlos, debemos mapearlos dentro del token a través de una serie de claims que se configuran dentro de Keycloak.

Para poder conceder accesos a través de roles, la aplicación deberá utilizar estos claims para calcular los roles de un usuario y, así, decidir el acceso a los recursos cuando se requiera.



Esto se puede trasladar a todo claim que se pueda mapear dentro de un token. Por lo cual, nuestra aplicación podría utilizar cualquier claim para garantizar el acceso. Para cada client, se puede adaptar qué claims se almacenarán en el token. Para esto, Keycloak provee de una funcionalidad llamada **protocol mappers**.

Particularmente no vamos a entrar, a lo largo de esta materia,e n profundidad con este tema. Sin embargo, si tienen ganas de investigar un poco más o ver su aplicación en Keycloak, pueden dirigirse al siguiente enlace de la documentación oficial enlace.