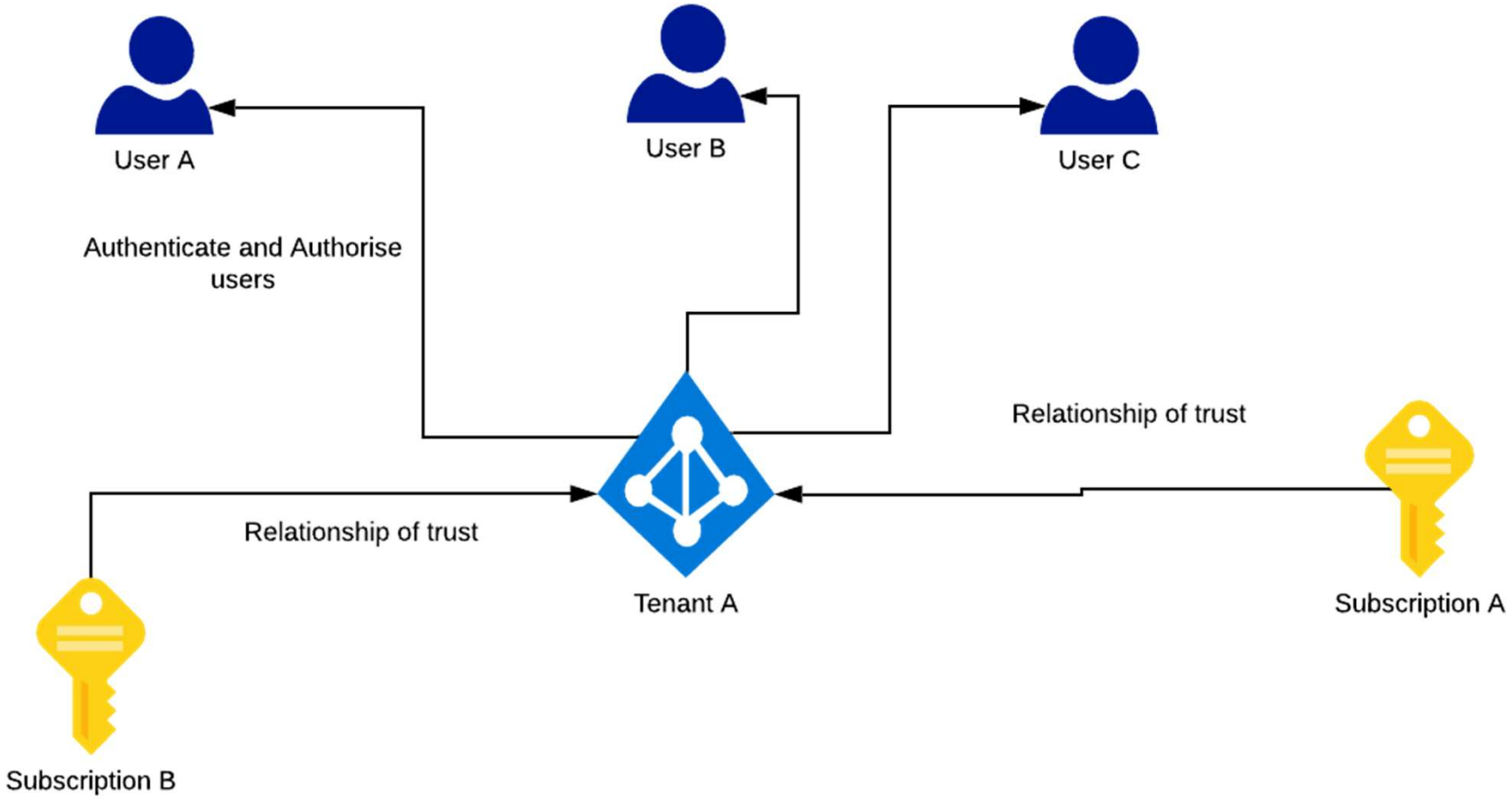
Azure Active Directory

Introduction



What are Security Principals?

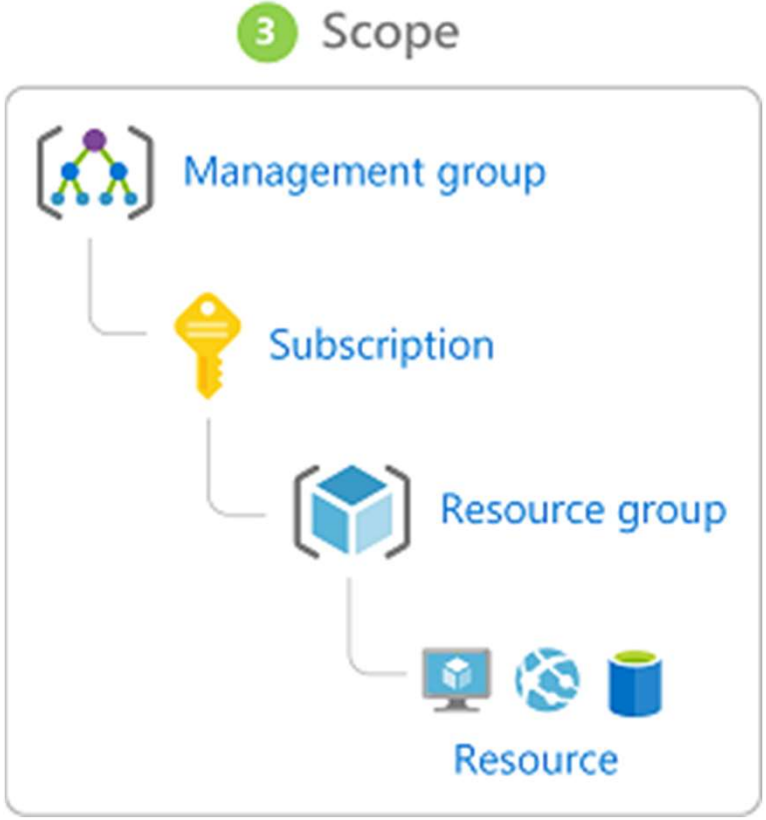
- User
  - Any user who has a profile in Azure Active Directory
- Group
  - Multiple users are assigned to a group
  - Roles can be assigned to groups, thereby impacting the users of that group
- Service principal
  - A security ID for apps
- Managed Identity
  - To help with credential management

Hands-On: Creating User and Group

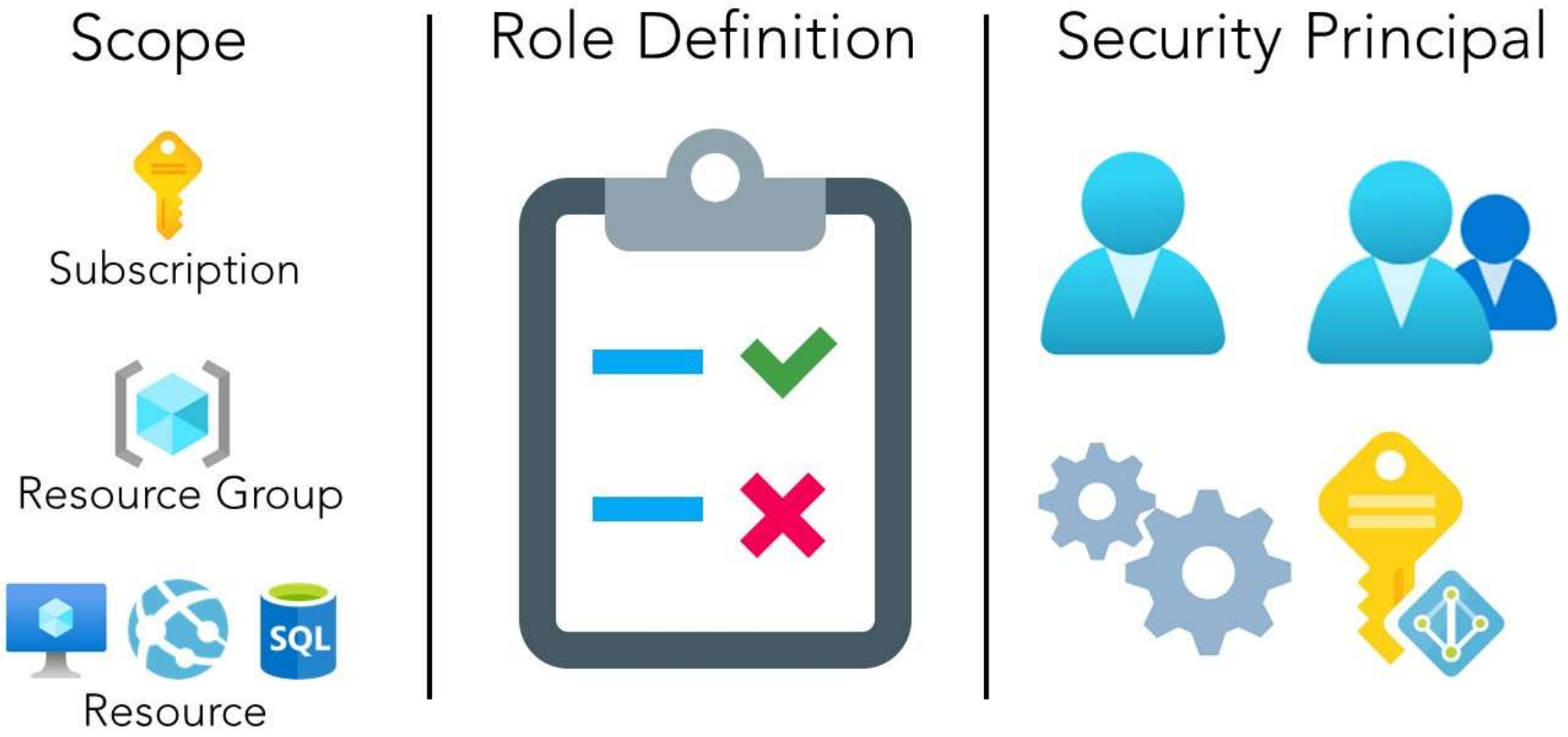
What is Role-Based Access Control?

- RBAC allows to assign permissions to users, groups, and applications
- For example
  - Global Admin can assign the role of **Virtual Machine Contributor** to **Janis** within the subscription
  - This grants **Janis** the right to create, delete, or modify any virtual machine within the subscription

Scope of RBAC



Scope, Role Definition and Security Principal



Azure Built-in Roles

- Owner
  - Has full access including
- Contributor
  - Has same access as owner other than delegation of access.
- Reader
  - Can view existing Azure resources

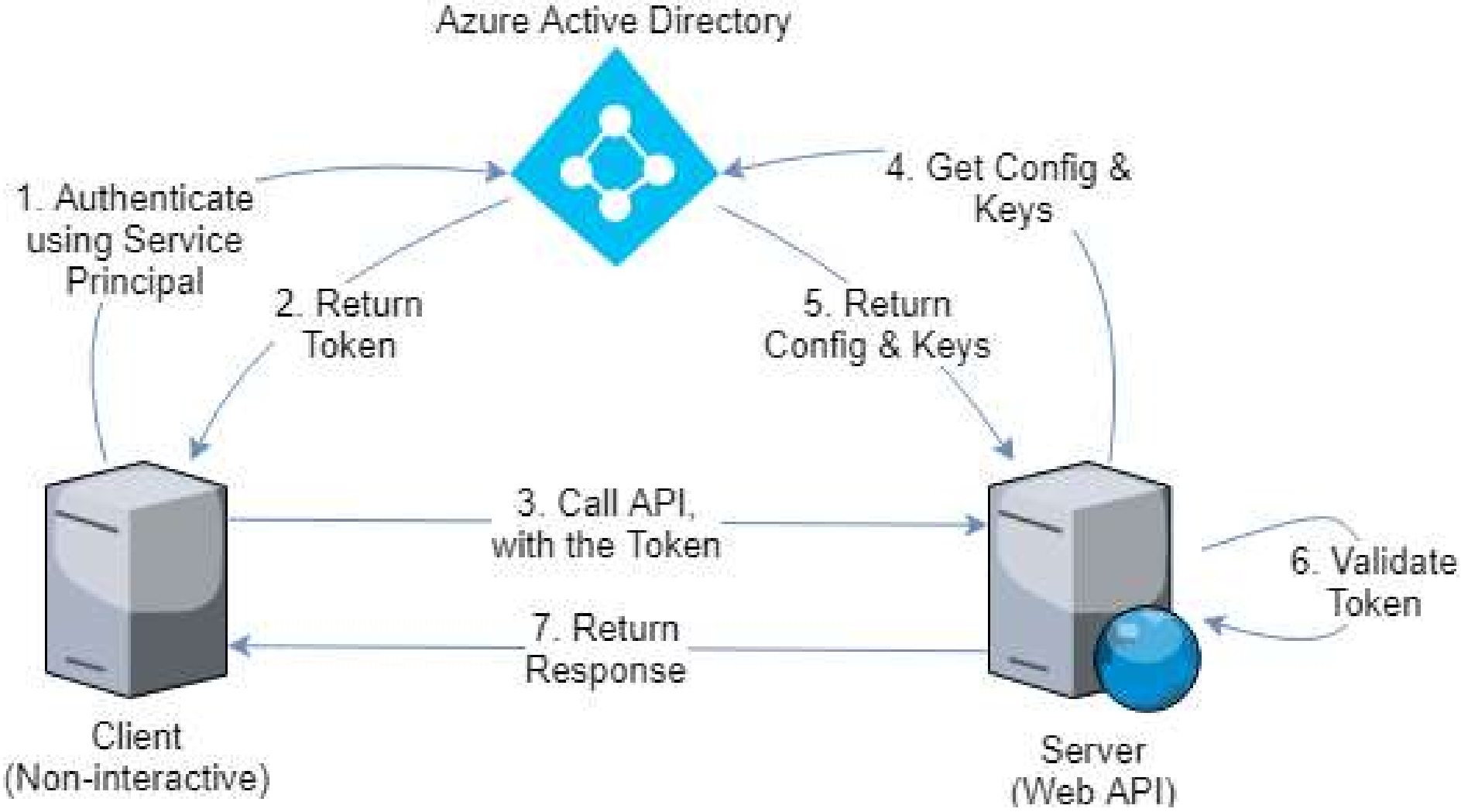
Hands-On: Assigning a Role to a User

Application Registration, Service Principal

Azure Service Principal

- A security identity used by
  - User-created apps
  - Services, and
  - Automation tools
- Think of it as a 'user identity' (login and password or certificate) with specific role
- It only needs to be able to do specific things, unlike a general user identity
- It improves security if you only grant it the minimum permissions level needed to perform its tasks.

Azure Service Principal




thanks