

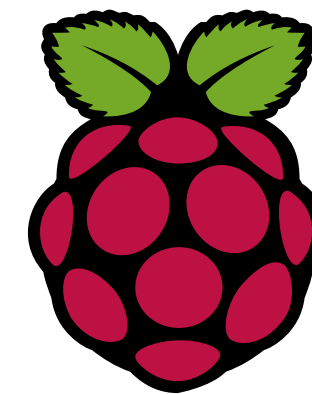
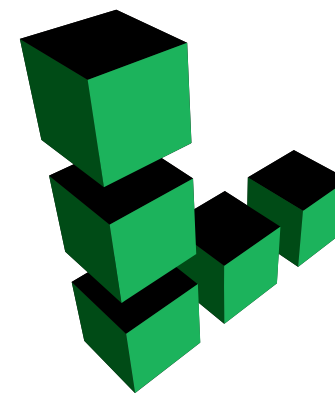
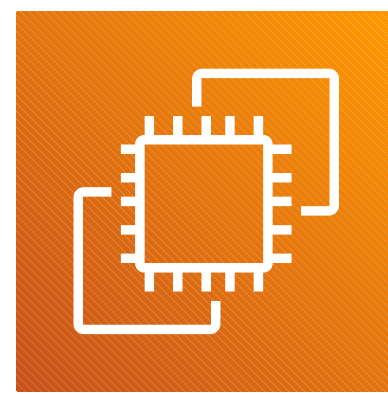
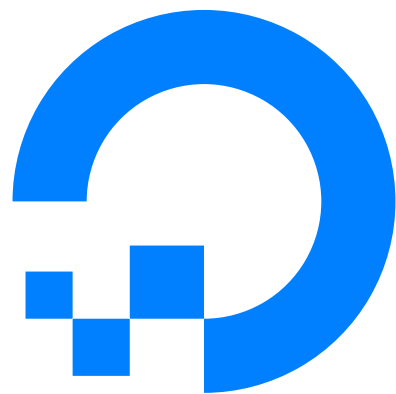
# **Module 1: The foundation**

## **Cloud setup & access**

# Cloud setup & access

## Prerequisites

- **Goal:** A secure environment before deploying code.
- **Providers:** DigitalOcean, AWS EC2, Linode, or Raspberry Pi.



# Cloud setup & access

## Prerequisites

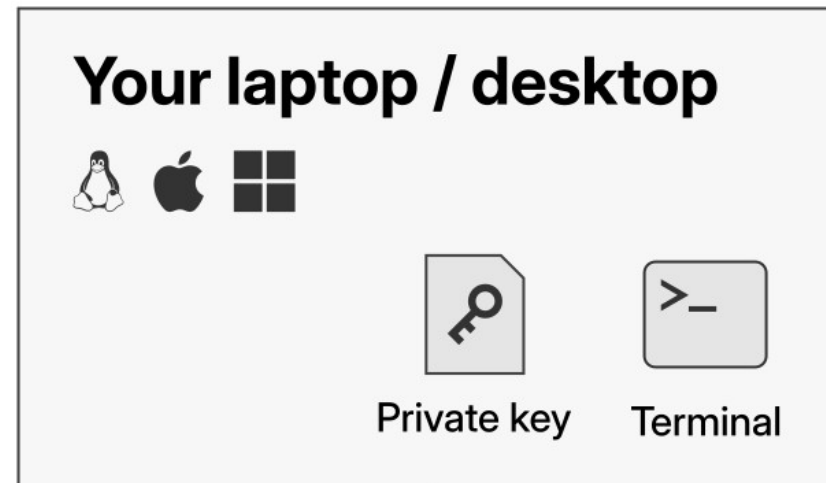
- **Goal:** A secure environment before deploying code.
- **Providers:** DigitalOcean, AWS EC2, Linode, or Raspberry Pi.

## Learning objectives

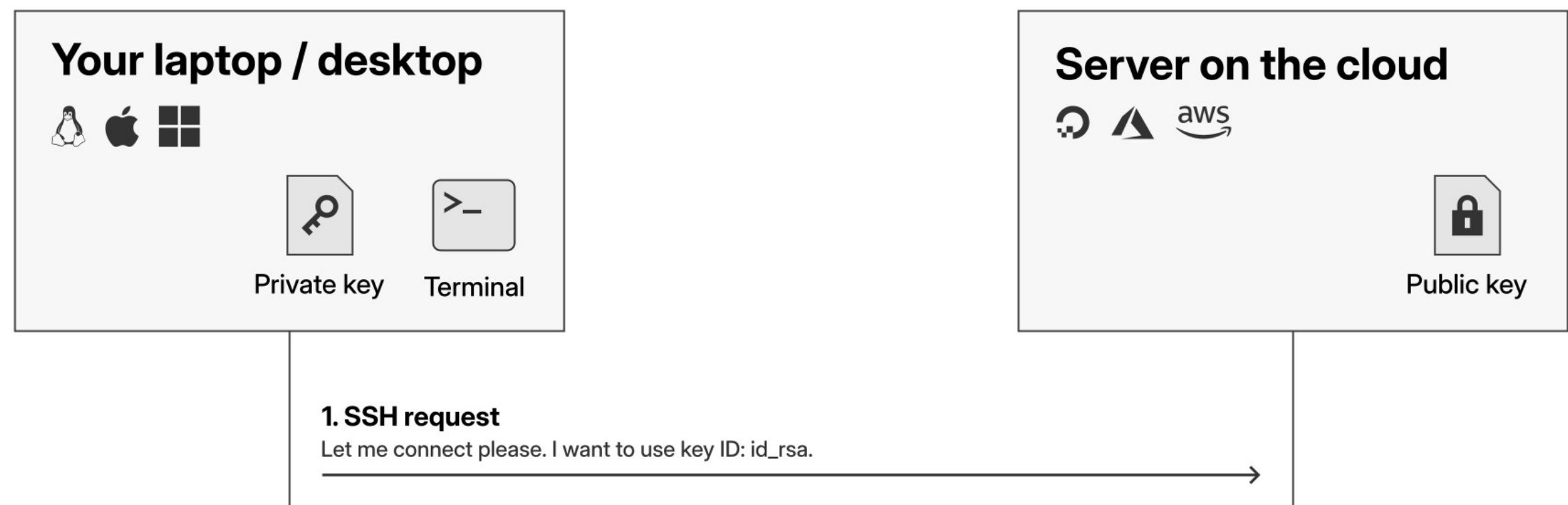
- Deploy a server running **Ubuntu 24.04 LTS**.
- Generate and configure **SSH Keys** ([Ed25519](#)).
- Understand the "**Lock & Key**" security model.
- **Security:** Disable password authentication completely.



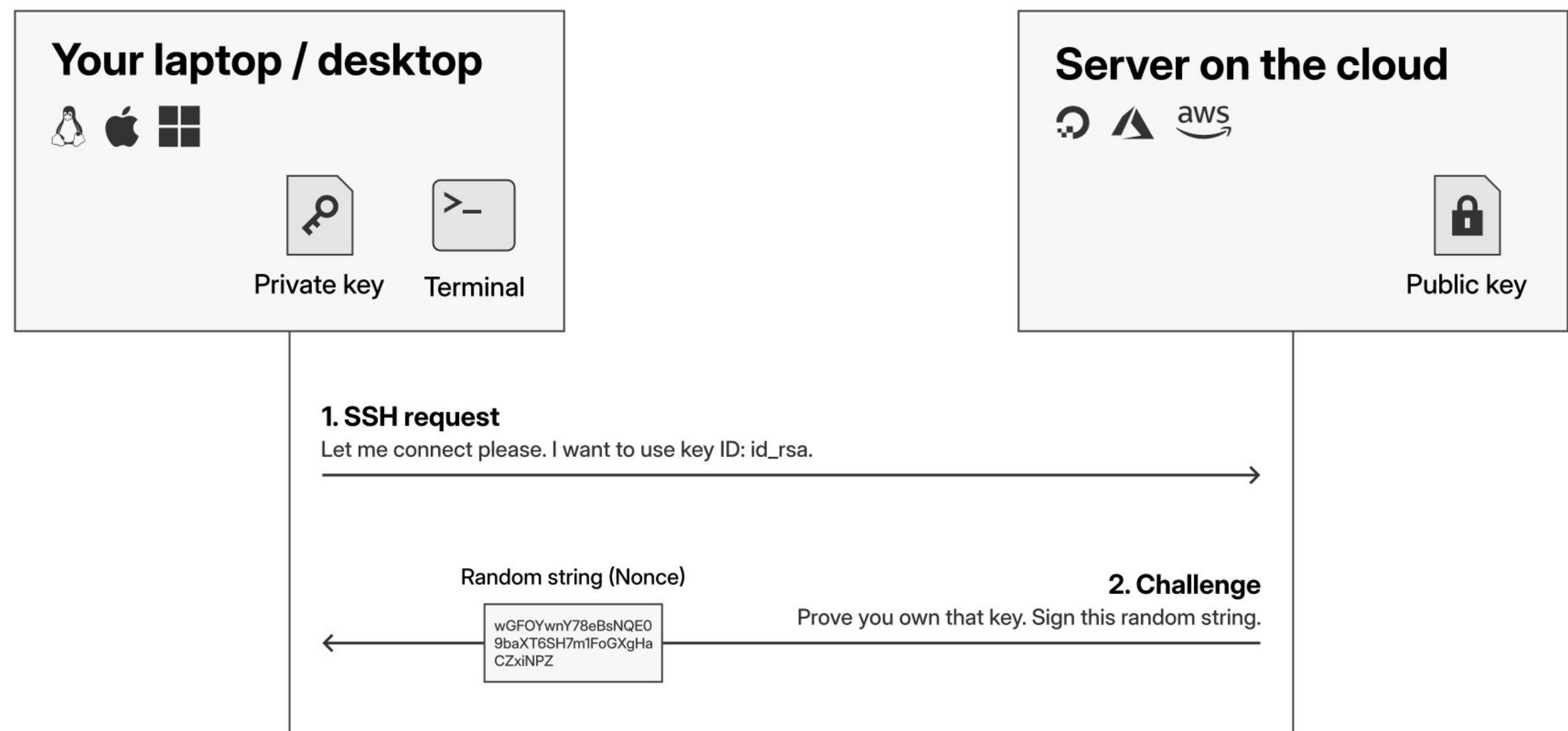
# How SSH keys work



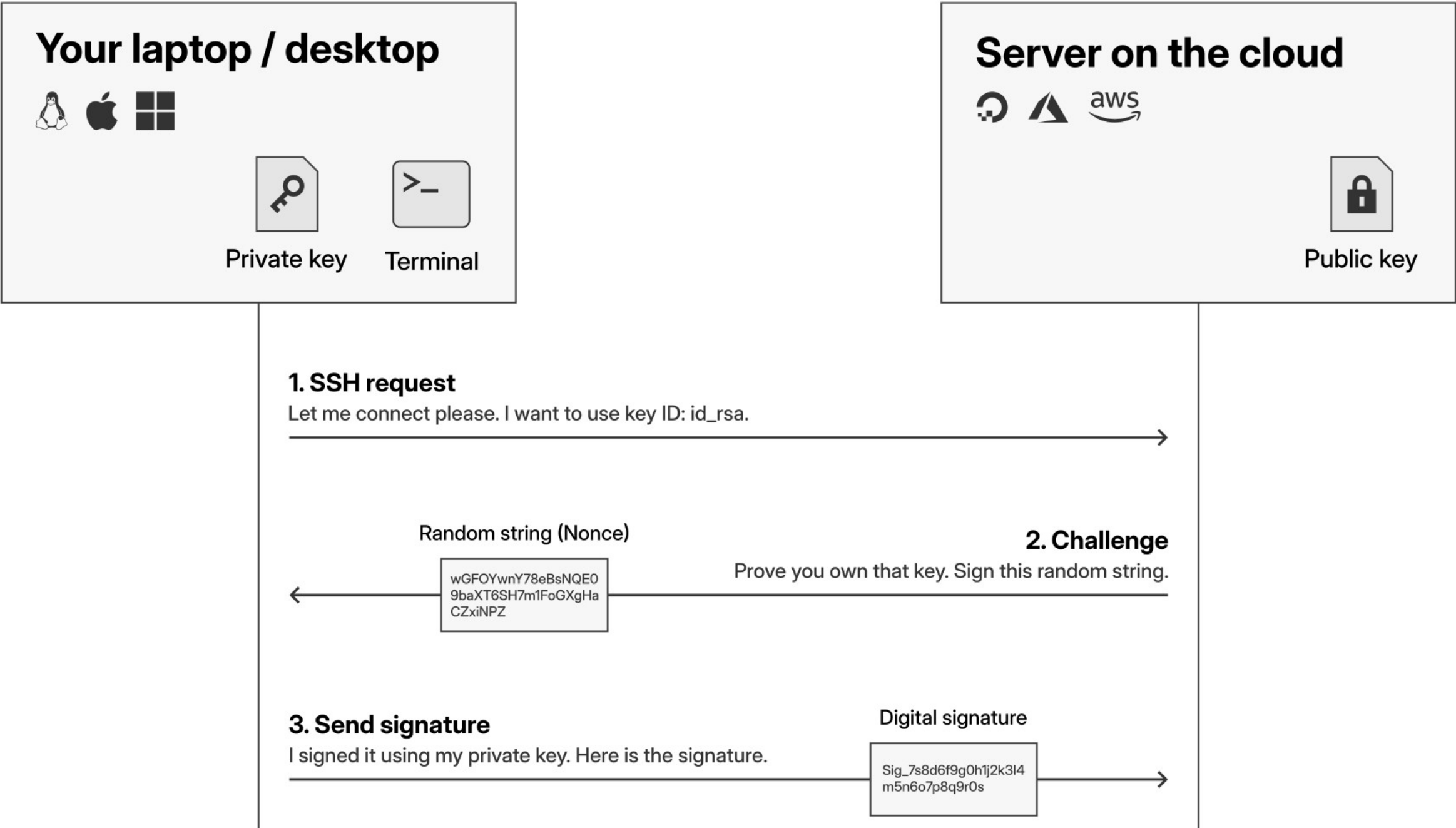
# How SSH keys work



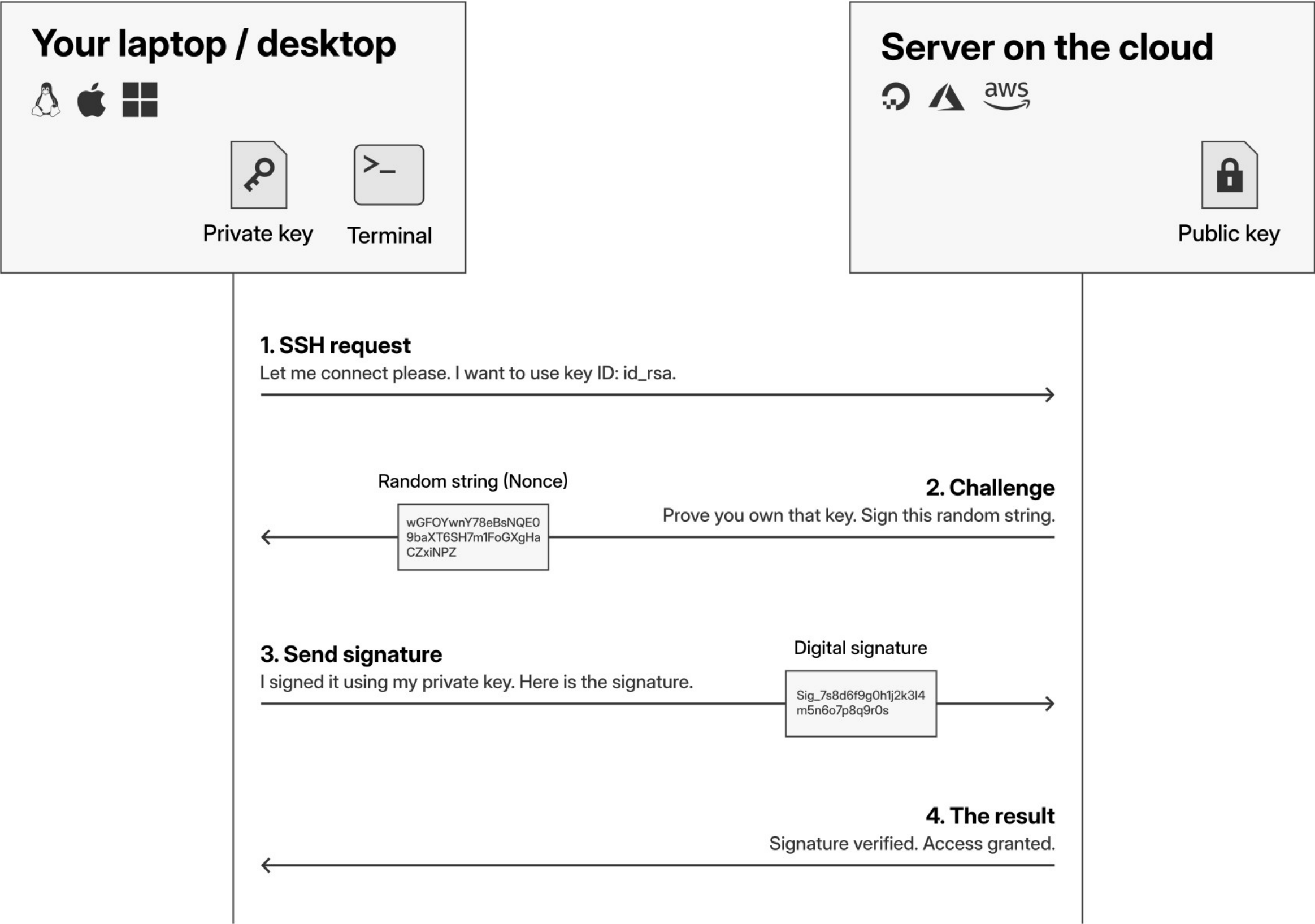
# How SSH keys work



# How SSH keys work



# How SSH keys work





# What is next?

- **Current status:** You now have a clean, secure Ubuntu server.
- **The risk:** The server is still exposed to the open internet.
- **Next steps:**
  - **Firewall configuration:** Setting up UFW (Uncomplicated Firewall).
  - **Brute force protection:** Installing Fail2Ban to block attackers.
  - **Emergency access:** How to use the recovery console.

