

## Lab 7 - PKI (public key infrastructure) & VPN (Virtual Private Network)



**The objective of this lab is to** understand the fundamentals of PKI and VPN, and learn how to observe encrypted traffic and VPN tunneling in practice. In particular, you have to configure a small PKI environment, generate certificates, and set up a VPN tunnel. You will also analyze traffic using Wireshark.

Send your report to: <csclass.dz@gmail.com>

Team information (one report by team)

- First Name Last Name: .....
- First Name Last Name: .....
- First Name Last Name: .....

Deadline: Wednesday, Dec 24, 2025 .

### **Part I: PKI Lab**

PKI enables secure communication using **digital certificates, public/private keys, and trusted authorities**. PKI ensures:

- Authentication (you are who you claim to be)
- Integrity (data is not altered)
- Confidentiality (data is encrypted)

#### **Examples of PKI usage**

- HTTPS (TLS/SSL)
- Email signing (S/MIME)
- VPN authentication

#### **Assigned Tasks: PKI**

1. **Generate a root CA**
  - Use OpenSSL or any similar tool
  - Create a self-signed root certificate
2. **Generate server and client certificates**
  - Create a server certificate signed by the root CA
  - Create a client certificate signed by the root CA
3. **Verify certificates**
  - Use OpenSSL commands to check validity
  - Inspect the certificate chain
4. **Observe PKI in action**
  - Use Wireshark to capture TLS handshake between a client and server using your certificates
  - Identify
    - Certificate exchange
    - Public key usage
    - TLS handshake messages

### Deliverables

- Used commands: text (detailed step by step, as done in previous labs)
  - For example, steps to generate CA, server, and client certificates
  - etc.
- Screenshot of certificate chain verification
- Wireshark capture with highlighted TLS handshake

### Part II: VPN Lab

A VPN establishes a **secure, encrypted tunnel** between a client and a server. VPNs protect traffic from eavesdropping and hide the real destination IP. Common VPN protocols: **OpenVPN, WireGuard, IPsec**.

### Examples of VPN usage

- Remote access to corporate networks
- Securing traffic on public Wi-Fi
- Bypassing geo-restrictions

### Assigned Tasks: VPN Lab

1. **Set up a VPN server**
  - Choose OpenVPN or WireGuard
  - Use previously generated PKI certificates for authentication (if using OpenVPN TLS mode)
2. **Configure a VPN client**
  - Connect the client to the VPN server
  - Verify IP change (e.g., `ifconfig` or `ip a`)
3. **Capture VPN traffic**
  - Use Wireshark on the client side
  - Identify
    - Encrypted tunnel traffic
    - VPN protocol (UDP/TCP)
    - Packet sizes and headers
4. **Test traffic through VPN**
  - Access a web service through VPN
  - Compare Wireshark capture **before** and **after** VPN connection

### Deliverables

- Used commands: text (detailed step by step, as done in previous labs)
  - For example, steps to configure VPN server and client
  - etc.
- Screenshot of VPN connection and IP change
- Wireshark capture showing encapsulated traffic (tunnel traffic)
- Brief explanation of how the tunnel protects data
- Compare encrypted vs unencrypted traffic

### Guidance Notes

- Pay attention to UDP vs TCP usage (include this point in your report)
- Observe overhead added by the VPN tunnel
- Try both TCP and UDP modes (if OpenVPN)

### **Part III: Reflection Questions Lab Report / Discussion**

- How does PKI support VPN authentication?
- What is encapsulation and tunneling in VPN traffic?
- How would HTTPS behave differently if VPN is active?