🔧 Шаг 1. Установка необходимых компонентов

sudo apt update

sudo apt install -y openssl ca-certificates

Если вы ещё не создали ЦС — создайте его

sudo mkdir -p /etc/pki/CA/{private,certs,newcerts,crl}

sudo touch /etc/pki/CA/index.txt

sudo echo 1000 > /etc/pki/CA/serial

sudo chmod 700 /etc/pki/CA/private

**Создайте корневой ключ и сертификат (RSA 4096, SHA256):**

sudo openssl req -x509 -new -nodes \

-keyout /etc/pki/CA/private/ca.key \

-out /etc/pki/CA/certs/ca.crt \

-days 3650 \

-sha256 \

-subj "/CN=AU-TEAM Root CA"

**Шаг 2. Создайте CSR для веб-сервера (если ещё не создан)**

# Ключ сервера (RSA 2048)

sudo openssl genrsa -out /etc/pki/CA/private/web.au-team.irpo.key 2048

# CSR

sudo openssl req -new \

-key /etc/pki/CA/private/web.au-team.irpo.key \

-out /etc/pki/CA/web.au-team.irpo.csr \

-subj "/CN=web.au-team.irpo"

# Ключ сервера (RSA 2048)

sudo openssl genrsa -out /etc/pki/CA/private/docker.au-team.irpo.key 2048

# CSR

sudo openssl req -new \

-key /etc/pki/CA/private/docker.au-team.irpo.key \

-out /etc/pki/CA/web.au-team.irpo.csr \

-subj "/CN=web.au-team.irpo"

**Шаг 3. Создайте конфигурационный файл для** openssl ca

Создайте /etc/ssl/openssl-ca.cnf:

[ ca ]

default\_ca = CA\_default

[ CA\_default ]

dir = /etc/pki/CA

certs = $dir/certs

crl\_dir = $dir/crl

new\_certs\_dir = $dir/newcerts

database = $dir/index.txt

serial = $dir/serial

RANDFILE = $dir/private/.rand

certificate = $dir/certs/ca.crt

private\_key = $dir/private/ca.key

default\_days = 30

default\_md = sha256

preserve = no

policy = policy\_anything

[ policy\_anything ]

countryName = optional

stateOrProvinceName = optional

localityName = optional

organizationName = optional

organizationalUnitName = optional

commonName = supplied

emailAddress = optional

[ server\_cert ]

basicConstraints = CA:FALSE

subjectKeyIdentifier = hash

authorityKeyIdentifier = keyid,issuer

keyUsage = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth

subjectAltName = @alt\_names

[ alt\_names ]

DNS.1 = web.au-team.irpo

DNS.2 = docker.au-team.irpo # если нужно для другого сертификата

**Шаг 4. Подпишите сертификат (ваша команда — но без ГОСТ)**

sudo openssl ca \

-config /etc/ssl/openssl-ca.cnf \

-in /etc/pki/CA/web.au-team.irpo.csr \

-out /etc/pki/CA/certs/web.au-team.irpo.crt \

-extensions server\_cert \

-days 30 \

-batch

sudo openssl ca \

-config /etc/ssl/openssl-ca.cnf \

-in /etc/pki/CA/docker.au-team.irpo.csr \

-out /etc/pki/CA/certs/docker.au-team.irpo.crt \

-extensions server\_cert \

-days 30 \

-batch

**Шаг 6. Настройка доверия на клиенте HQ-CLI**

Скопируйте корневой сертификат:

Изображение выглядит как текст, Шрифт, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Шаг 7. Настройка Nginx на HTTPS**

Пример конфига для web.au-team.irpo:

sudo mkdir -p /etc/nginx/ssl

sudo cp /etc/pki/CA/certs/web.au-team.irpo.crt /etc/nginx/ssl/

sudo cp /etc/pki/CA/private/web.au-team.irpo.key /etc/nginx/ssl/

sudo chown root:root /etc/nginx/ssl/\*

sudo chmod 600 /etc/nginx/ssl/\*.key

sudo nginx -t && sudo systemctl reload nginx