

SSL Certificate Check

Background

Secure Sockets Layer (SSL) is widely used to establish encrypted connections over the internet. SSL certificates help verify the identity of the remote server. In this task, you'll connect to a given hostname over HTTPS (port 443), retrieve its SSL certificate, and check for required fields.

Task

Your task is to:

- Establish a secure connection using SSL to a known web server.
- Retrieve the server's SSL certificate.
- Validate that the certificate contains required fields such as 'subject' and 'issuer'.
- Extract the Common Name (CN) from the certificate's subject field.

Input

There is no input. The server details are hardcoded as:

- Hostname: www.google.com
- Port: 443

Output

Common Name (CN): www.google.com

Certificate has all required fields: ['subject', 'issuer']

Constraints

- Use the ssl module and socket to establish the secure connection.
- Use getpeercert() to retrieve the certificate in a dictionary format.
- Extract the CN by converting the 'subject' field to a dictionary and accessing the 'commonName'.

Implementation guide

You must implement the following function:

```
def get_ssl_certificate(hostname, port):  
    # Establish SSL connection and retrieve peer certificate  
    pass
```

In your main function:

- Connect to www.google.com on port 443.
- Retrieve the certificate.
- Print:
 - A message indicating whether the fields 'subject' and 'issuer' are present
 - The Common Name (CN) from the 'subject' field.