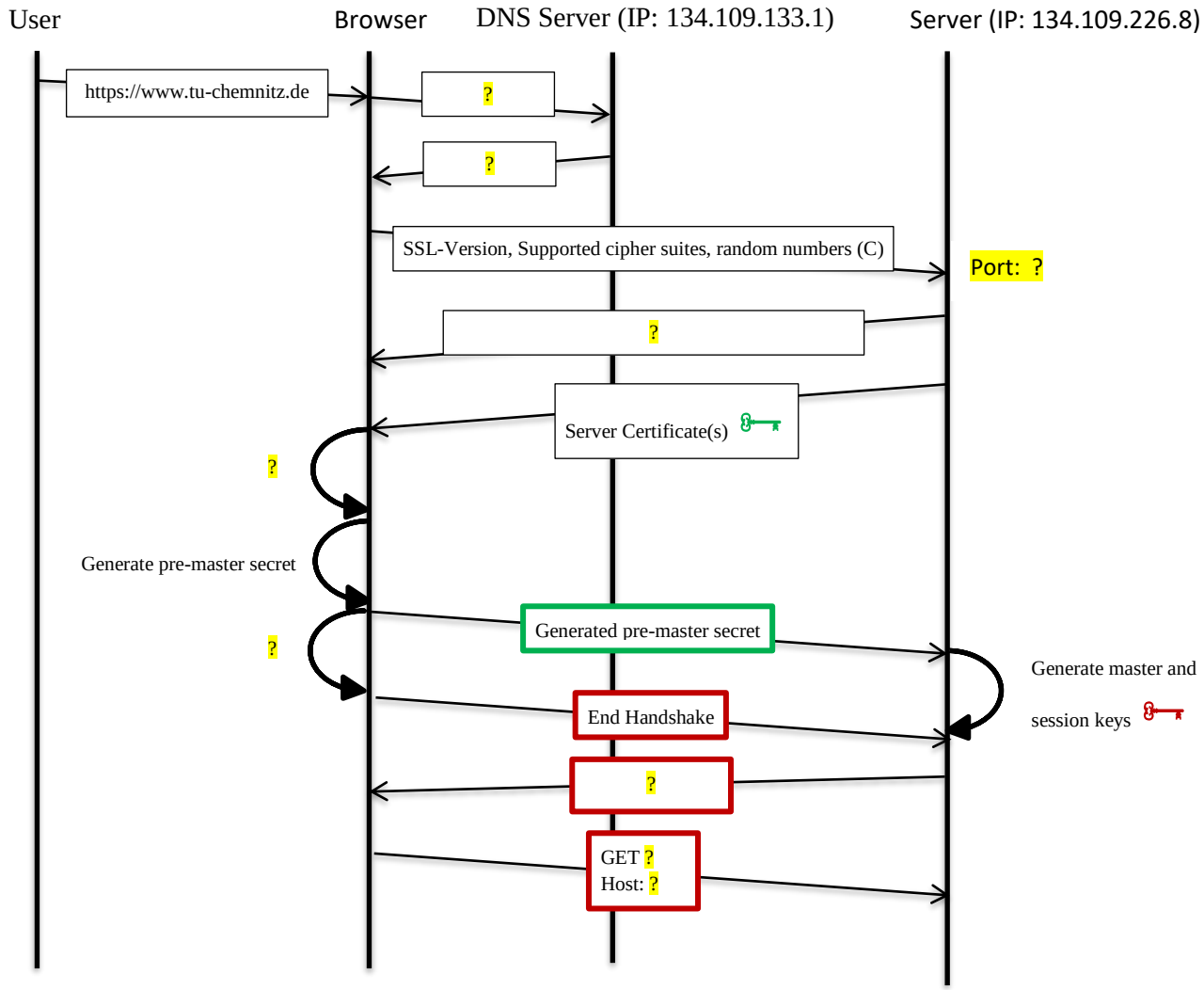
SVS | Exercise 7

Task 1

Vervollständigen Sie das folgende Sequenzdiagramm, das beschreibt, was Ihr Browser macht, wenn Sie die Seite *https://www.tu-chemnitz.de* aufrufen.

Complete the following sequence diagram, which describes, what your browser is doing while you are requesting the page https://www.tu-chemnitz.de.



a. Welche Ziele werden mit SSL/TLS verfolgt? Welche Sicherheitslücken gibt es trotz des Einsatzes von SSL/TLS?
b. Wie unterscheidet der Server, welches Zertifikat ausgeliefert werden soll, falls mehrere virtuelle Hosts existieren?

a. Which goals does SSL/TLS have? Which risks exist despite of usage of SSL/TLS?
b. How does server decide, which certificate should be shown, if several virtual hosts exist?

Task 2

Informieren Sie sich über die HTTP Digest Authentifizierungsmethode[1].

1. Inwiefern ist sie besser als HTTP Basic?
2. Welche Risiken sind damit trotzdem verbunden?
3. Was würde ein Client als Antwort auf die folgende Server-Nachricht übermitteln, falls sein Nutzername „Max“ und Passwort „Secure123“ sind?

Inform yourself about the HTTP Digest authentication method[1].

1. How is it better than HTTP Basic?
2. Which risks do still exist?
3. What would a client send as a response to the following server message, if his username would be „Max“ and his password - „Secure123“?

Request:

```
GET /index.html HTTP/1.1
Host: localhost
```

Response:

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Secured Area",
nonce="aer95b7fg2dd2hhe8b11d0f6f7afb0c14v"
Content-Length: 0
```

Task 3

Informieren Sie sich darüber, wie die Public Key-Authentifizierung im SSH Authentication Protocol[2] funktioniert. Konfigurieren Sie den SSHD Dienst auf einem Server (oder auch auf dem lokalen Rechner) so, dass dieser die Public Key-Authentifizierung erlaubt:

1. Für einen Nutzer erzeugen Sie ein Schlüsselpaar:

ssh-keygen -t rsa

2. Übertragen Sie den öffentlichen Schlüssel auf den entfernten Server:

ssh-copy-id –i .ssh/id_rsa.pub {user}@{server}

3. Konfigurieren Sie den SSH-Dienst zur Verwendung der Public Key-Authentifizierung
   a. Entfernen Sie die Kommentarzeichen in */etc/ssh/sshd_config* in den Zeilen mit *PublicKeyAuthentication yes* und AuthorizedFiles *.ssh/authorized_keys*
   b. Starten Sie den Dienst neu: */etc/init.d/sshd restart*
4. Testen Sie die Anmeldung mittels der soeben erzeugten Schlüssel:

ssh {user}@{server}

Inform yourself about the way, how Public Key-Authentication in SSH Authentication Protocol[2] works. Configure the SSHD service on a server (or the local machine), so that it enables Public Key Authentication:

1. Create a key pair for a user:

ssh-keygen -t rsa

2. Transfer the public key to the server:

ssh-copy-id –i .ssh/id_rsa.pub {user}@{server}

3. Configure the SSH service to use the Public Key Authentication:
   a. Remove the comment symbols in /etc/ssh/sshd_config in the rows with *PublicKeyAuthentication yes* and *AuthorizedFiles .ssh/authorized_keys*
   b. Restart the service: */etc/init.d/sshd restart*
4. Test the authentication using the newly created keys:

ssh {user}@{server}

---

[1] http://en.wikipedia.org/wiki/Digest_access_authentication
[2] http://tools.ietf.org/html/rfc4252