Note: For the questions below, feel free to use online resources as needed. If necessary, you can create diagrams to aid explanation. Please ***cite*** *your references properly.*

1. (20 points) A bank recently changed its website name from *www.bank32.com* to *www.bank48.com*. To cut costs, the bank wants to reuse the existing certificate from *www.bank32.com*. Would that be possible? If possible, how does it work? (Hint: Do some research for ***wildcard certificates.***)

No, it would not. A certificate is tied to a domain name. If the domain name changes, the certificate becomes invalid for the new domain. Wildcard certificates would not be valid as they cover subdomains (eg. bank.bank32.com) , not different domains entirely.

2. (30 points) A TLS client program typically uses the server's certificate to authenticate the server during a TLS handshake. But what about the reverse direction?

   Please do some research and answer the following:

   1) Does TLS support server-to-client authentication? If so, what is this feature called? How does it work?
      Yes, TLS supports server-to-client authentication, and it is called Mutual TLS (mTLS) or client authentication.

      How it works:
      1. The normal handshake happens (server begins by presenting its certificate)
      2. The server sends a CertificateRequest message, which tells the client to prove who they are
      3. The client presents a client certificate, signed by a CA
      4. The server validates the client's certificate
      5. The handshake finishes and the session is secured

   2) Provide one real-world example or use case where client authentication in TLS is implemented. Describe:
      - What type of application or service uses it?
      - Why is client authentication necessary in that context?
      - What form does the client credential typically take?

One real world use case of TLS client authentication is corporate VPNs. Internal company resources may use a VPN to allow those not on the corporate network to access protected resources. Client authentication is necessary as systems need a machine-level identity. The client credential typically takes an X.509 certificate on the user's device that is usually issues by the company's own CA.