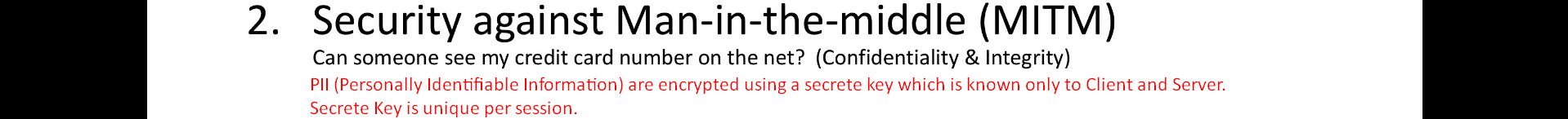
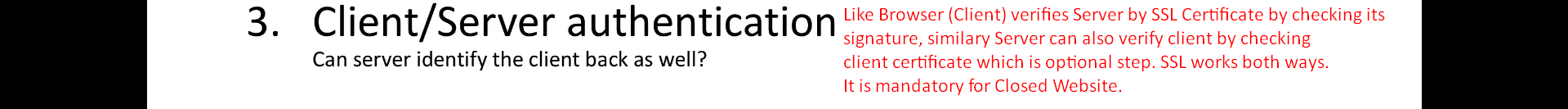
1. Let’s first discuss about these before going into technicality.
   1. Why do we need SSL Certificate?
   2. Let’s see what problems it solves in internet communication.
2. We will cover 4 major benefits of SSL certificates and see what problems, each of them solves.



1. **Source Identify Verification**:  
   
   1. When logging in to a bank site, we want to make sure that the site is the actual bank site to avoid any possibility of someone presenting you a similar looking page under the same domain name.  
      The **attackers** usually do this by intercepting the traffic to and from the genuine site and your machine.
   2. **SSL helps to identify if the website**, we are accessing is genuine or not.  
      This is done **cryptographically by the browser**.
   3. The browser verifies **the signature in the SSL Certificate** to check its genuineness.
   4. Once it is verified, the browser will add a **VISUAL GREEN PADLOCK** **SEAL** on the left side of the address bar.
   5. This is how we know, the site we are accessing is actually what it claims to be.
2. **Security Against Man-In-The-Middle (MITM)**
   1. This is second advantage of SSL.
   2. Protecting sensitive data online is very essential to build customers trust.
   3. Protecting PII (Personally Identifiable Information) like credit card number, SSN, Password, DOB, Medical Records, Phone Number, Sexuality etc. need to be kept secure under various audit standard laws.
   4. **Communication over SSL** makes sure that the data transfer is **encrypted** with a secret key known only to the client and server.  
      **This secret key is unique per session**.
3. **Client/Server Authentication**:  
   
   1. **3rd Benefit**.
   2. A server can also identify a client back.
   3. SSL works both ways.
   4. Like a browser verified the identity of a server/website, similarly, server can verify a client through **client certificate**.
   5. Client Certificate is an **optional step** in SSL Communication.
   6. Mandatory for **Closed Website** where the web server wants to identify the clients accessing it.  
      But in general, in the case of internet, there is no client certificate involved.
4. **Non-Repudiation:**
   1. During the **SSL connection establishment**, once the browser verifies the signature produced in the SSL Certificate from the server, the server is said to be authenticated.
   2. From that point onwards, whatever communication happens, it is definitely from the server and the server can not repudiate/deny it any time in the future.