𝗪𝗼𝗿𝗸𝗶𝗻𝗴 𝗼𝗳 𝗦𝗦𝗟 𝗶𝗻 𝗡𝘂𝘁𝘀𝗵𝗲𝗹𝗹 !  
  
𝗦𝘁𝗲𝗽 𝟭: 𝗘𝘀𝘁𝗮𝗯𝗹𝗶𝘀𝗵 𝗔𝘂𝘁𝗵𝗼𝗿𝗶𝘁𝘆  
- Initiate the process by setting up your own Certificate Authority (rootCA) along with a private key. This rootCA acts as a trusted entity to validate your certificate.  
  
𝗦𝘁𝗲𝗽 𝟮: 𝗖𝗦𝗥 𝗚𝗲𝗻𝗲𝗿𝗮𝘁𝗶𝗼𝗻  
- With your server's private key, generate a Certificate Signing Request (CSR) that includes essential details like your domain name and company information.  
  
𝗦𝘁𝗲𝗽 𝟯: 𝗖𝗲𝗿𝘁𝗶𝗳𝗶𝗰𝗮𝘁𝗲 𝗜𝘀𝘀𝘂𝗮𝗻𝗰𝗲  
- Use the CSR and your CA's certificate to create an SSL certificate. This SSL certificate is what enables secure connections.  
  
𝗦𝘁𝗲𝗽 𝟰: 𝗖𝗲𝗿𝘁𝗶𝗳𝗶𝗰𝗮𝘁𝗲 𝗖𝗿𝗲𝗮𝘁𝗶𝗼𝗻  
- You now have a self-signed SSL certificate ready to be implemented, ensuring encrypted connections to your server.  
  
𝗦𝘁𝗲𝗽 𝟱: 𝗔𝗽𝗽𝗹𝗶𝗰𝗮𝘁𝗶𝗼𝗻 𝗜𝗻𝘁𝗲𝗴𝗿𝗮𝘁𝗶𝗼𝗻  
- Integrate the self-signed SSL certificate with your application. This ensures that the data transferred between the server and client is encrypted.  
  
𝗦𝘁𝗲𝗽 𝟲: 𝗦𝗲𝗰𝘂𝗿𝗶𝘁𝘆 𝗪𝗮𝗿𝗻𝗶𝗻𝗴  
- Be aware that browsers will show a warning for self-signed certificates as they are not verified by a third-party authority.  
  
-----------------------------  
  
📌 Save this post for later and follow [Hina Arora](https://www.linkedin.com/in/ACoAABpDUJ0BowkjKeWqbn5vmgqWb1KgpzPW6qI) for more insightful information.

Activate to view larger image,

