Let us assume that IITH going to have many web services inside the campus which would be accessed among the IITH community. In this case, we may not need to have server certificates to be issued by a public Certificate Authority, we can have our own Certificate Authority to have secured services. This assignment is about creating such infrastructure and services by completing the following four tasks.

Task 1 (10 Points) - Creating a Public Key Infrastructure (PKI) for IITH: Let us have one root CA for IITH who would certify the intermediate CA for each department (Admin, CSE, EE, etc.). When each department wants to host their web servers then can get their server certificate signed by the intermediate CA of their own department. All the IITH community can configure their system to trust the IITH root CA. You need to create this PKI for IITH. You can use any cloud services such as Google Cloud and create VMs for each entity (root CA, CSE CA, EE CA, etc.). Server certificates for each department can be certified by only the respective intermediate CAs.

Task 2 (10 points) - Creating a webserver with HTTPS support: The web server inside a particular department creates their own certificate and get it signed by the department's intermediate CA. The web server should allow only HTTPS connections to it. Configure the web server accordingly and configure the browser to trust the root CA that you have created in Task 1. Host a web service that collects user profile for registration for a particular service. The user suppose to fill a form with some personal information. You need to show using wireshark that the connection between the client and server happens over HTTPS. You can either use a public cloud service such as Google Cloud or your own laptop/desktop.

Task 3 (40 Points) - Secure Peer-to-Peer application using PKI: Let us assume that the IITH community wants to create a secure application (e.g., chat application / gaming / file transfer / etc.) using the PKI of IITH in Task 1. You can pick up any application of your choice. You need to use the PKI of IITH to get the user certificates and use SSL based communication between the users. Create your application using socket programming using SSL socket and show that the communication between the users is secure.

Task 4 - (10 Points) Extending the application among multiple PKIs: If you assume that each IIT has its own PKI and they trust each other. Create a mechanism in PKI infrastructure so that the application that you have created in Task 3 can work among the community of different IITs. You can demonstrate this by creating 2 PKIs where users certified by different PKIs are able to use the application developed in Task 3.

Report (10 Points): The report should be a detailed project report and self sufficient to understand what you have done. You can add screenshots to show the working of the system.

Deliverables: You need to submit all your source codes and a detailed report in a single .zip file with filename as your roll number. All the tools and softwares used should be given with reference.

Evaluation: All the code submitted will be checked for plagiarism. Any plagiarism issue will be dealt with the department plagiarism policy. The assignment will be evaluated by the TAs on a scheduled date and time. If you do not appear for evaluation the will be treated as not submitted.

Late Submission Policy: 20 % penalty for each late day submission.