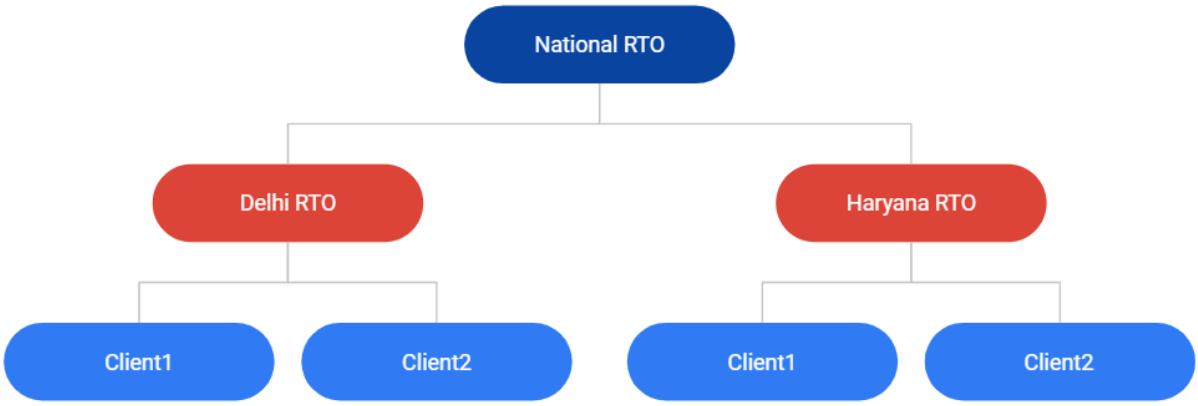
Assignment 4

Network security
Hritik Goel (2018148)
Dushyant Panchal (2018033)
Project #2: Verification of Driver's License




```
license = json.dumps({
    "type": 1,
    "signingAuthority": "DELHI TRANSPORT AUTHORITY",
    "cert": (1, 3, 4, 11, 7, 8, 19, 17, 0, 13, 18, 15,
    "sign": 5
})
```

MODULES

Backend.py

- Class RSA - copied from the previous assignment.
- Class TransportAuthority - provides backend utilities for transport authority servers.

Server.py

- Server app for different tier transport authorities to run.

Client.py

- Client app for traffic policemen to connect in order to verify license.

Others

- Defined a server config to run the example of National RTO managing Delhi and Haryana RTOs.

- A managing RTO is responsible for communicating kPU of its dependents with each other.
- A simple cert_file.py example for signing of a license by an RTO / transport authority.

QUESTIONS

Q1. What is the information to be supplied by the driver to the police officer? And what information is sought and obtained by the police officer from the transport authority?

A1. Driver needs to provide the original driving license digitally signed by a certain transport authority.
Police officer needs to check whether the provided license is valid or signed by any RTO, so he/she will obtain the public key of the RTO that signed the license (even in case the client and traffic men are of different states) and decrypt the signature and match with the original information.

Q.2. Would you need a central server that has the correct and complete information on all drivers and the licenses issued to them?

A.2 No, we may not always need the central server in case the RTO of different cities are directly connected. If in case, we may need the central server, it doesn't need to store the information of all the drivers. The central server just needs to craft the certificate, containing the public key of the requested RTO.

Q.3. Is date and time of communication important?

A.3. Date and time of communication are important to prevent replay attacks.

Q.4. In what way are digital signatures relevant?

A.4 Digital signatures help in authentication, integrity and non-repudiation of original information of license holders by the traffic men. As, traffic men or RTO (having the public key corresponding to the license-issuing RTO) can decrypt the signature and compare it with the original information, to judge whether the client is having the right to drive or license valid.

Q.5 Does one need to ensure that information is kept confidential? Or not altered during 2-way communication?

A.5 No information is not required to be confidential. However, the information must not be altered during the course of communication.

6. Which of these, viz. confidentiality, authentication, integrity and non-repudiation is/are relevant?

A.6 All are essential except the confidentiality. Also, digital signatures help in ensuring the authentication, integrity and non-repudiation.