Report

Nikunj Singhal(2018249)
Aman kumar Gupta(2018217)

Ans 1. The driver gives the following information to the police officer:

a. The license number.
b. Name
c. Issue date
d. Validity date
e. Digital Signature

The police officer parses the data in valid format and encrypts it with his private key and sends it to the verification server along with signature.

Ans 2. Since we are using digital signatures which are signed by a secret private key of the transportation authority, we do not need to maintain any central server with all data for the purpose of verification.

Ans 3. Yes, date and time are important in the context of a driver's license since the license is only valid till the expiration date.

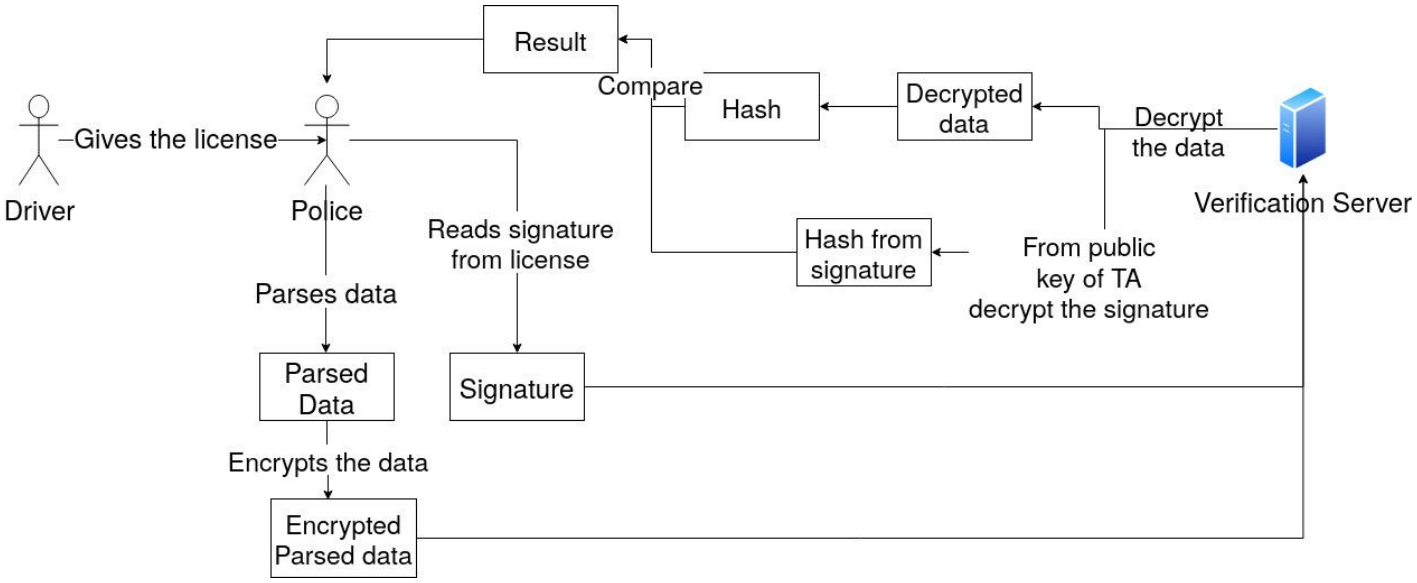
Ans 4.Digital signatures reduce the risk of duplication or alteration of the document itself. Digital signatures **ensure**

that signatures are verified, authentic and legitimate. Digital signatures are used to meet three important goals of information security: integrity, authentication, and non-repudiation.

Ans 5. Yes, we need to make sure that information is kept confidential as it contains information of the driver's license which can be replicated if leaked. We need to make sure that the information is not altered so we can be sure that a third party did not maliciously alter the driver's license information to a valid license information which results in the license to be verified in case it is not. We do this by encrypting the data by police officer's private key.

Ans 6. Confidentiality, authentication, integrity and non-repudiation are all important during the two way communication. We achieve this by encrypting the communication between police officer and verification server via private key cryptography. Where anyone can encrypt the data but only verification server can decrypt it.

Architecture:



Outputs:

```
parsed data: 21092019Dl34321iONikunj21092023
Issued license with data: {'name': 'Nikunj', 'license_no'
: 'Dl34321iO', 'issued_on': '21092019', 'valid_till': '21
092023'} signature: 583 118 583 1579 1359 111 1699 30 583
 118 583 111 583 23 1699 803 2013 593 803 1579 1460 593 3
0 23 1699
verifying license with data: {'name': 'Nikunj', 'license_
no': 'Dl34321iO', 'issued_on': '21092019', 'valid_till':
'21092023'} and signature: 583 118 583 1579 1359 111 1699
 30 583 118 583 111 583 23 1699 803 2013 593 803 1579 146
0 593 30 23 1699
verification status: True
##########################################
verifying license with data: {'name': 'Aman', 'license_no
': 'Dl34321iO', 'issued_on': '21092019', 'valid_till': '2
1092023'} and signature: 583 118 583 1579 1359 111 1699 3
0 583 118 583 111 583 23 1699 803 2013 593 803 1579 1460
593 30 23 1699
verification status: False
```