Verification of driving license

Important points:

- RSA encryption, decryption, key generation is used
- Server has police public key
- Police has server public key
- Server has two sets of key, one for encrypted_code and another for sending and receiving messages
- Server uses the same key ‘K1’ for encryption and decryption of code in the license.

Implementation:

- When a driver registers for a license, the driver gets his license with personal details like name, DOB, expiry date and an encrypted code(using private key of K1).
- During verification, police sends the (details, encrypted_code) using encryption(police private key) to server- ensure authentication
- Server receives encrypted message and decrypts it(police public key)
- Server verifies by comparing decrypted code(using public key of same key K1) and sends verification status in encrypted message(server private key of key K2) - ensure confidentiality
- Police receive messages and decrypts(server public key of key K2) to see verification status.

1. 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 server in the transport authority?
Ans-The driver would provide their driver's license card to the police officer. This card may contain personal information such as name, date of birth, address, license number, etc. The police officer would then query a server in the transport authority to verify the authenticity of the license and retrieve any additional relevant information such as the license status, validity period, and any associated restrictions or endorsements.

2. Would you need a central server that has the correct and complete information on all drivers and the licenses issued to them?
Ans- Yes, a central server would be necessary to store and manage the correct and complete information on all drivers and the licenses issued to them. This central server would serve as the authoritative source of information that can be accessed by police officers on the go.

3. In what way are digital signatures relevant?
Ans-Digital signatures can play a crucial role in ensuring the authenticity and integrity of the information exchanged between the driver, the police officer, and the central server. The driver's license information can be digitally signed by the transport authority before being issued to the driver. When the police officer queries the central server, the response can also be digitally signed to prevent tampering or forgery.

4. Does one need to ensure that information is kept confidential? Or not altered during 2-way Communication?
Ans-Both confidentiality and integrity are important aspects of the communication between the police officer and the central server. Confidentiality ensures that sensitive information exchanged during the verification process is protected from unauthorized access. Integrity ensures that the information remains unchanged during transit between the parties involved.

5. Which of these, viz. confidentiality, authentication, integrity and non-repudiation is/are relevant?
Ans- Confidentiality: Relevant to protect sensitive information exchanged during the verification process.
Authentication: Relevant to ensure that both parties (the driver and the central server) can verify each other's identity.
Integrity: Relevant to ensure that the information exchanged is not tampered with or altered during transit.
Non-repudiation: Relevant to provide evidence that the driver presented a valid license and that the central server provided accurate information in response to the query.

https://www.canva.com/design/DAGBzfaDrwQ/xR83xvvTYPM8fnwI7keM0g/edit?utm_content=DAGBzfaDrwQ&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton