On-the-go verification of Driver's License

Programming Assignment 4
CS350, Monsoon 2020

Aditya Singh Rathore
2018007

Jaspreet Saka
2018237

November 24, 2020

Abstract

Typically a police officer looks at the driver's license card physically and simply assumes that the license, together with the information it contains, was issued by the "transport authority", and none else. However it is not difficult to copy, alter or produce a fresh plastic card. In this project, we use Digital Signatures to create a system to verify on-the-go a driver license card, when shown to a police officer on road or elsewhere. The idea can be used to verify any indentity card.

1 Identity Card

1.1 Biological Identity

A requirement for the system to be correct is that a biological identity, most likely a fingerprint be stored along with other information in the database.

Here is an example. Suppose there is a 30 year old man X and he steals License of another $30ish$ man Y and superimposes his photo. Now, when X shows his ID card, the policeman will be able to verify that the card

is valid (as it belongs to Y). However, there is no way, he will be able to verify without further investigation that this man is X and not Y.

Naturally, the policeman has to carry a fingerprint scanner with him. The cost and size of equipment is not much of a issue given that they carry a *Challan Machine* with them.

Another way can be image. The server can send image back to the policeman. Or a policeman can send the image to the server.

The fact is that for the system to be correct, we need some sort of biological identification.

1.2 The Server

1.2.1 Nature of Server

The server need not be a centralized server *physically*. However, we need the information to be accessible to everyone.

The interface over which policeman asks for verification should have access to all the information and not some subset of it.

1.2.2 Information Stored

The server will have personal information, validity of card and the biological identity stored with itself.

2 Process

2.1 Overview

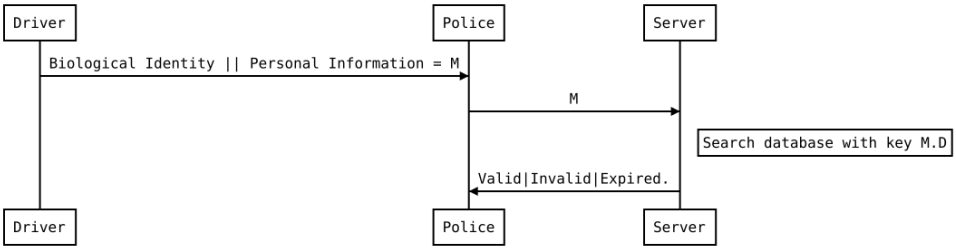

Figure 1: Overview of Communication involved

- Driver shows Card to Police.
- Police extracts personal information and biological information.
- Police sends information to trusted Server.
- Server verifies if card is **valid** or **invalid** or **expired**.

2.2 Server

- Server finds Tuple ω using index $M.D$ where M is message and D is index.
- If ω is empty (Not present), Server responds **invalid card**.
- If ω is present, server matches biological identity and personal information.
- If match is $False$, server responds **invalid card**.
- If matcn is $True$, server checks for expiry date of card.
- If card is expired, server returns **expired**.
- Server returns **Valid card**.

3 Digital Signatures

We use **RSA** digital signatures. to verify police and server.

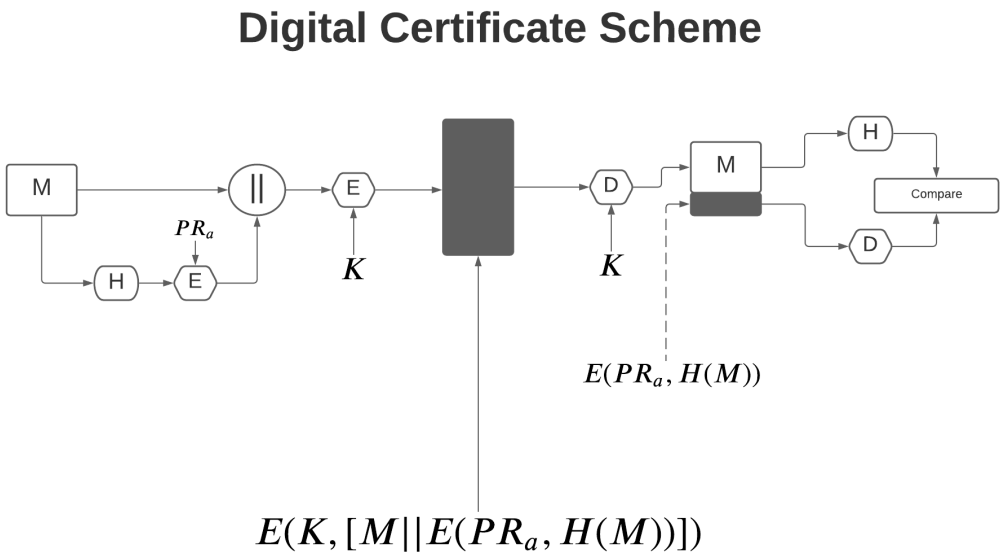

Figure 2: Complete process

3.1 Sender

Message to be signed is input to a hash function that produces a secure hash-code of fixed length.This hashcode is encrypted using senders private key to form signature. Both message and signature are encrypted and transmitted.

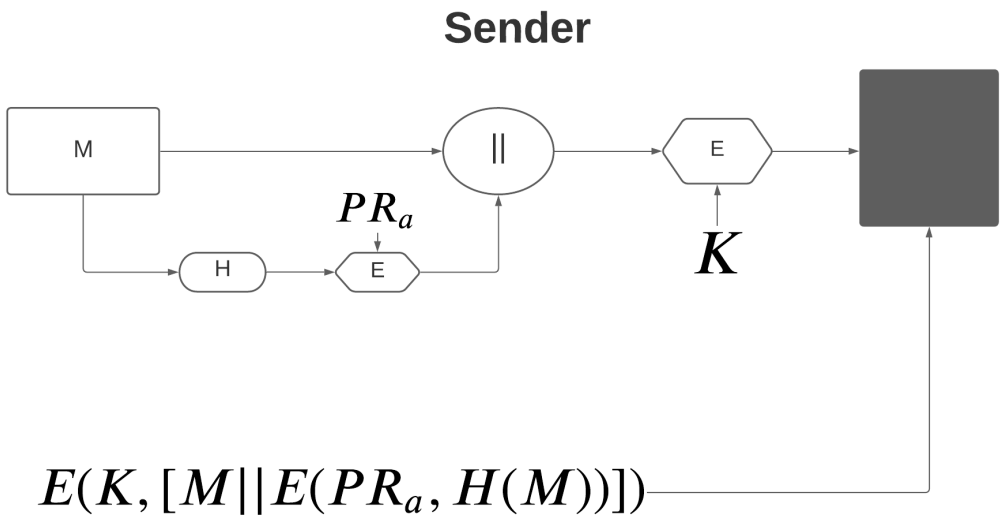

Figure 3: Sender side of digital certificate

3.2 Reciever

The reciever takes the message and decrypts it. It then takes message from decrypted text and also the encrypted hashcode. It calculates the hash of message and compares it with decrypted hash. Only sender knows the orivate key, only sender could produce valid signature.

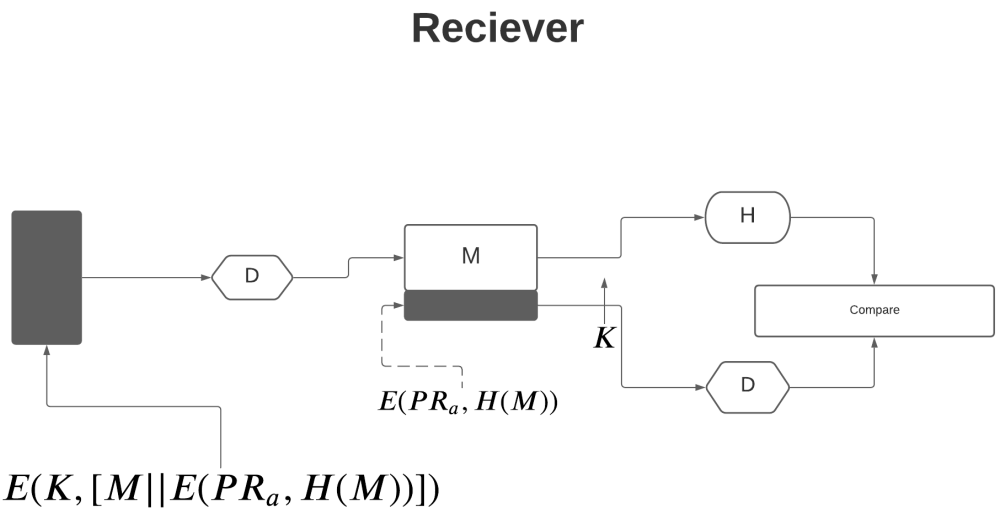

Figure 4: Reciever side of digital certificate

4 Assignment

4.1 Questions

4.1.1 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 transport authority?

Information supplied is Driver's personal info and biological identity. Information sought is whether card is valid or not.

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

We need a central interface that has correct and complete information on all drivers and the licenses issued to them. (*See server above*)

4.1.3 Is date and time of communication important?

Yes. This is because licenses have a validity period.

4.1.4 In what way are digital signatures relevant?

Digital signatures help authenticate the policeman and server both to each other. A Digital signature gives the receiver reason to believe the message was sent by the claimed sender

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

Yes, otherwise policeman can be fooled by man-in-the-middle attacks.

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

All of them are important.

- **Confidentiality:** Informatio has to be confidential (see above).
- **Authentication:** Property that a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.
- **Integrity:** If the message is tempered, it can lead to license frauds.
- **Non-Repudiation:** Neither police or server should be able to deny that they have not sent a license for verification or the validity of license. Otherwise, it can lead to frauds.

  If any of the above is not met, it can lead to frauds.