TÉCNICO LISBOA

Master Degree in Computer Science and Engineering

Segurança Informática em Redes e Sistemas 24/25

MOTOR IST

Group T27

Diana Goulão | IST1 102531

Mafalda Fernandes | IST1 102702

Miguel Sol | IST1 102710

POINTS OF DISCUSSION

01 Introduction

02 Built infrastructure

03 Secure document format

04 Secure channels and key distribution

05 Security requirements and challenge

06 Demonstration

TÉCNICO LISBOA

INTRODUCTION
OVERVIEW

- Car
- Types of client:
  - Owner
  - Mechanic
  - Manufacturer
- Client operations
- Restrictions

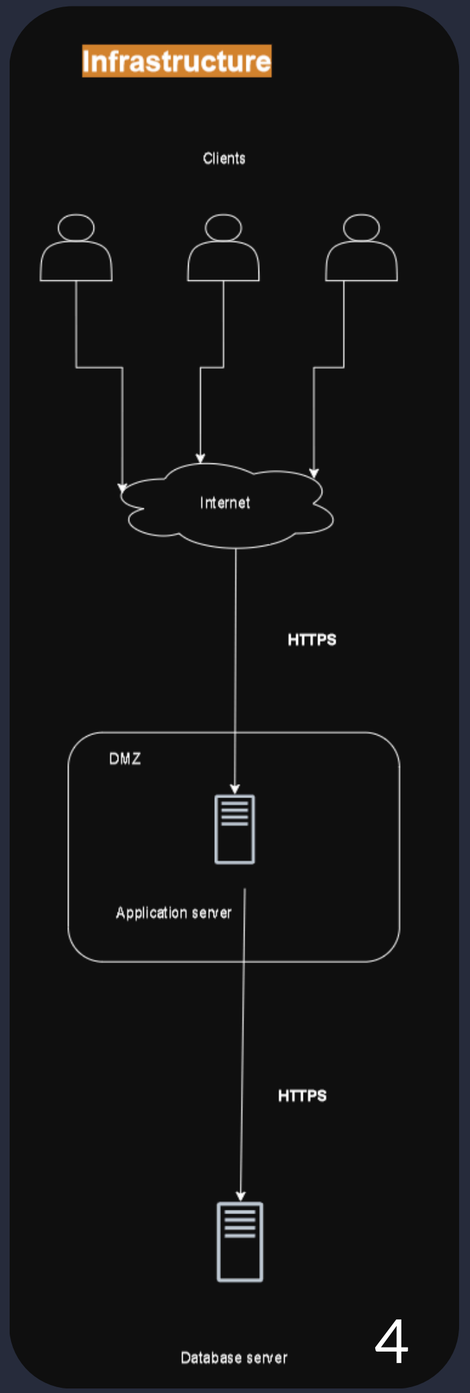
TÉCNICO LISBOA

BUILT INFRASTRUCTURE

DataBase Server

Application Server

Clients Server



TÉCNICO LISBOA

SECURE DOCUMENT FORMAT
OVERVIEW

- **Objective:** Ensure data confidentiality, integrity, and authenticity;
- **Development:** Built in Java using Java Crypto;
- **Main Use:** Encryption of car configurations during communications;
- **Features:** CLI support and JSON Object manipulation;

SECURE DOCUMENT FORMAT

PROTECT COMMAND

- **Encryption:** AES for content, RSA for secret key integrity.
- **CLI & Integration:** Results saved to a path or included in the transmitted message.
- **Protect operations**:
  - protecting only with a symmetric key
  - protecting a symetric key with an asymmetric key
  - protecting content encrypted with a symmetric key and the key with an asymmetric key

SECURE DOCUMENT FORMAT

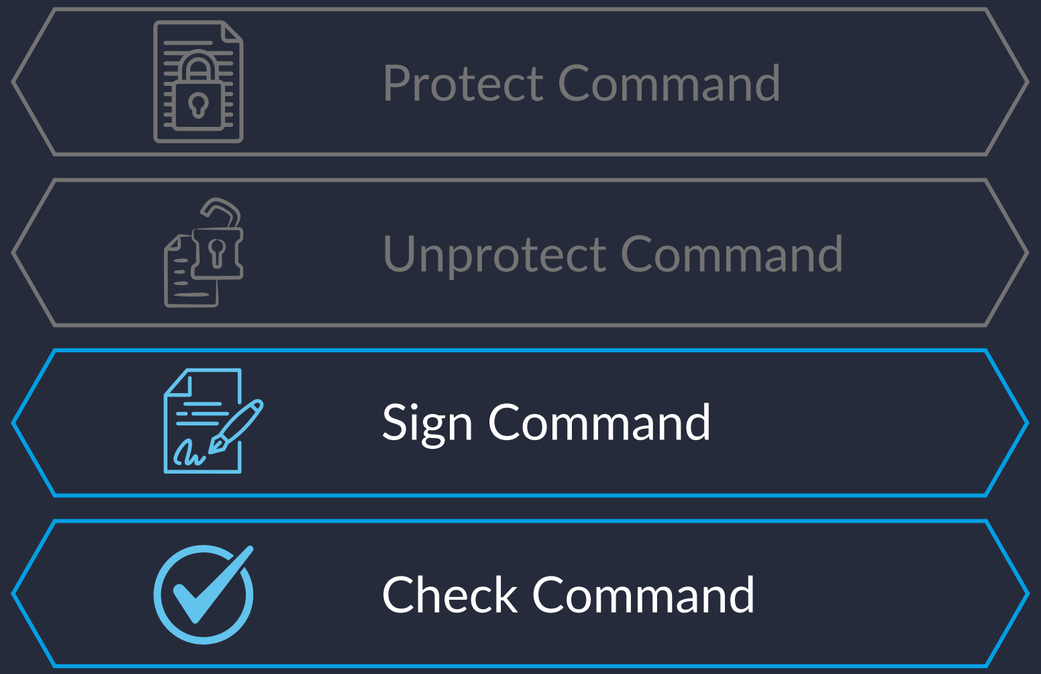
UNPROTECT COMMAND

- **Decryption:** Secret key to decrypt content, asymmetric key to decrypt secret key.
- **CLI & Integration:** Results saved to a path or returned.
- **2 modes:**
  - Unprotect with only asymmetric (RSA)
  - Unprotect with asymmetric (RSA) and symmetric (AES)

SECURE DOCUMENT FORMAT

SIGN AND CHECK COMMANDS

- **Sign:** Private Key and JSON object, also uses “SHA256withRSA” algorithm.
- **Check:** Public Key and JSON object.
- **CLI & Integration:** Results saved to a path or returned.



TÉCNICO LISBOA

SECURE CHANNELS
KEY DISTRIBUTION

SECURE CHANNELS

KEY DISTRIBUTION

- **Car Key Analogy:**
  - Symmetric key (car.key) mimics a real car key;
  - sharing is physical or assumes possession.
- **Key Distribution:**
  - Private keys for users; server holds public keys for verification.
  - Symmetric key only shared physically, ensuring security.

SECURE CHANNELS

SECURE CHANNELS

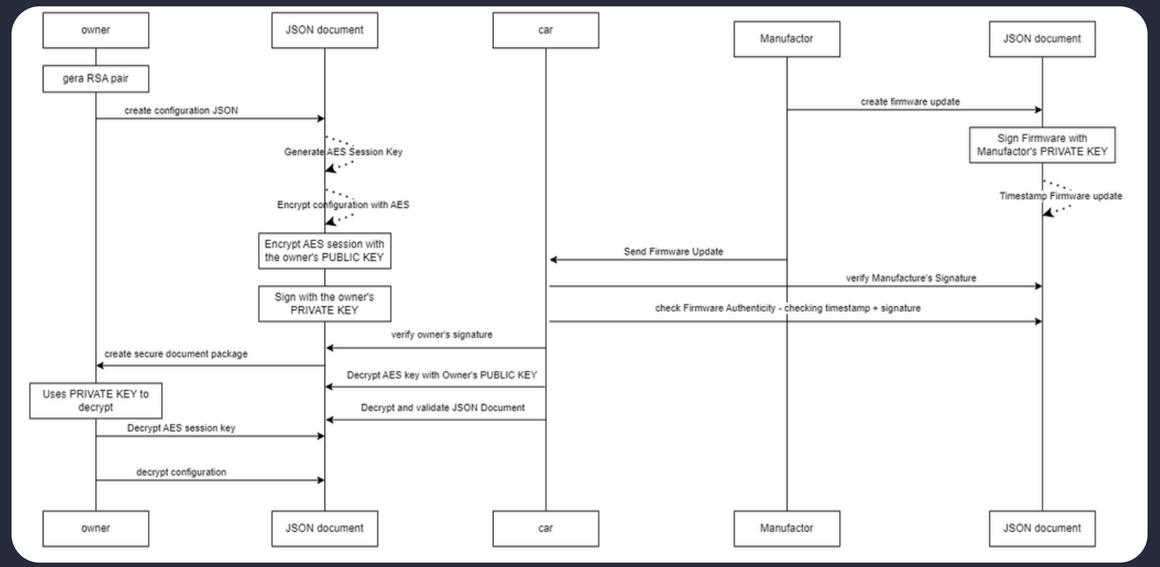
- **TLS:**
  - **Confidentiality**
  - **Data Integrity**
  - **Authentication**
  - **Protection against attacks like Man in the Middle and Replay attacks**
- **Ficticious CA**

KEY DISTRIBUTION

TÉCNICO LISBOA

SECURITY REQUIREMENTS
OVERVIEW

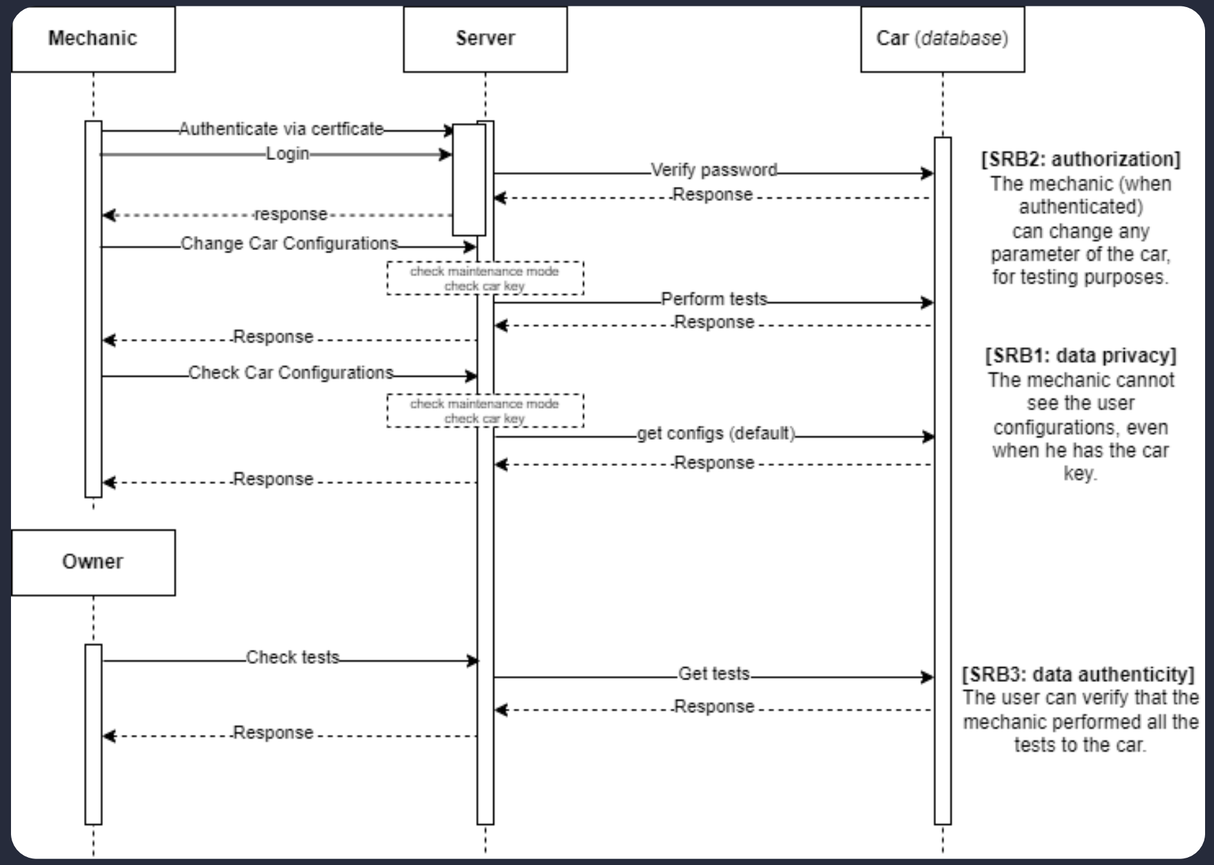
- [SR1: Confidentiality] The car configurations can only be seen by the car owner.
- **[SR2: Integrity 1] The car can only accept configurations sent by the car owner.**
- [SR3: Integrity 2] The car firmware updates can only be sent by the car manufacturer.
- [SR4: Authentication] The car manufacture cannot deny having sent firmware updates.



TÉCNICO LISBOA

SECURITY CHALLENGE
OVERVIEW

- **[SRB1: data privacy]** The mechanic cannot see the user configurations, even when he has the car key.
- **[SRB2: authorization]** The mechanic (when authenticated) can change any parameter of the car, for testing purposes.
- **[SRB3: data authenticity]** The user can verify that the mechanic performed all the tests to the car.



TÉCNICO LISBOA

DEMONSTRATION

LOGIN

Client

```
Welcome to the System!
Please select your client type:
1. User
2. Manufacturer
3. Mechanic
4. Exit
1
You selected: User
Please enter your password: VyXeCrCxpEQDInzt5yAf
Please enter your id:
owner1
Successfully Authenticated
```

Database

```
[INFO]
[INFO] --- exec-maven-plugin:1.6.0:java (default-cli) @ databa
$2a$10$eMatFjbBuBaP7Tpw.ACaYOKqANYL0A/WESyeeDwFrMEvSaR75BvsC
```

```
t27motorist_db=> select * from owner;
 ownerid |      name      |                          password_hash
---------+----------------+------------------------------------------------------------
 owner1  | João Silva     | $2a$10$eMatFjbBuBaP7Tpw.ACaYOKqANYL0A/WESyeeDwFrMEvSaR75BvsC
 owner2  | Maria Oliveira | d3d9446802a44259755d38e6d163e820
(2 rows)
```

Server

```
Peer certs: [Ljava.security.cert.X509Certificate;@61324cf9
Connected entity's certificate subject: CN=DB,O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Database connected.
Peer certs: [Ljava.security.cert.X509Certificate;@577cfa3b
Connected entity's certificate subject: CN=USER,O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Waiting for authentication
user Authenticated
```

DEMONSTRATION

CHANGE CAR CONFIG

Client

- Insert data not encrypted
- Send encrypted data

```
select what you want to change:
1. AC
2. Seats
3. Finish and send new configuration
4. Cancel all changes
Your choice: 2

Select seat position to change:
1. Seat position 1
2. Seat position 3
3. Go back
Your choice: 1
Enter value for Seat position 1: 6
Seat position 1 value added: 6

Select seat position to change:
1. Seat position 1
2. Seat position 3
3. Go back
Your choice: 3

Select what you want to change:
1. AC
2. Seats
3. Finish and send new configuration
4. Cancel all changes
Your choice: 3
Owner changed the config to: {"configuration":{"seat":[{"pos1":"6"},{"pos3":"1"}],"ac":[{"out1":"1234"},{"out2":"123
tyh+VRK7UsIrzuM60SbCkrDlP0ZGoab5Di0jwyZqFojunhFuKSRHbm5Dc16i6bqRXoE3d3pWbrMGhR7xB6bEddpHx+dOoIhpfYFXYwWZxMM3SEN7z5I3
BdXOf+WzHbA+ODiiKwun/KXRSG73s/OYXNZug+QHIy12SNS/RCRIwLtc/KOw2HJh0MbQoWTBh3WB8nwKWCpK3qYEGkthX9oJ7w0Aw=="}
Encrypted new config to send to database: {"configuration":"Moadj8ErGD86DWuZ7O4k23z7ueRr1smbwmkaoMh2QX8nb3GMTVhLP86n
5mlpuqnqkOZCueXGZJp6ygOApS/SJqCfLyCek2+pIwc30DwMtyh+VRK7UsIrzuM60SbCkrDlP0ZGoab5Di0jwyZqFojunhFuKSRHbm5Dc16i6bqRXoE3
mJZOz5XyVHidoB4gRi0bwXPllGajuc4JQ74TpWhjBLae90HjBdXOf+WzHbA+ODiiKwun/KXRSG73s/OYXNZug+QHIy12SNS/RCRIwLtc/KOw2HJh0Mb(

Changing car configuration...
Configuration changed successfully.
```

Database

- Received encrypted confinguration
- Store encrypted configuration

```
New config to set:
{"configuration":"Moadj8ErGD86DWuZ7O4k23z7ueRr1smbwmkaoMh2QX8nb3GMTVhLP86nm87
c30DwMtyh+VRK7UsIrzuM60SbCkrDlP0ZGoab5Di0jwyZqFojunhFuKSRHbm5Dc16i6bqRXoE3d3p
ae90HjBdXOf+WzHbA+ODiiKwun/KXRSG73s/OYXNZug+QHIy12SNS/RCRIwLtc/KOw2HJh0MbQoWT
```

```
 configid | carid | is_default | userid |         timestamp          |
                                                                                              configuration_details

----------+-------+------------+--------+----------------------------+------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------
        1 | car1  | t          | owner1 | 2024-12-01 08:05:00        | {"configuration":"Moadj8ErGD86DWuZ7O4k2wzcqXsRPIKE9hM6gpesyE98fciPbyb+8P
FRwRHaKI="}
        2 | car2  | t          | owner2 | 2024-12-05 10:15:00        | {"configuration":"Moadj8ErGD86DWuZ7O4k2wzcqXsRPIKE9hM6gpesyE98fciPbyb+8P
FRwRHaKI="}
        3 | car1  | f          | owner1 | 2025-01-08 00:03:39.557348 | {"configuration":"Moadj8ErGD86DWuZ7O4k23z7ueRr1smbwmkaoMh2QX8nb3GMTVhLP8
HJq057WY=","signature":"SvWFO5mlpuqnqkOZCueXGZJp6ygOApS/SJqCfLyCek2+pIwc30DwMtyh+VRK7UsIrzuM60SbCkrDlP0ZGoab5Di0jwyZqFojunhFuKSRHbm5Dc16i6bqRXo
7z5I3UrohG/AWqEG/fx/V/uRG5JMqmJZOz5XyVHidoB4gRi0bwXPllGajuc4JQ74TpWhjBLae90HjBdXOf+WzHbA+ODiiKwun/KXRSG73s/OYXNZug+QHIy12SNS/RCRIwLtc/KOw2HJh0M
(3 rows)
```

RESULTS
CONCLUSION

WHAT WE HAVE LEARN

- How to implement security in the exchange of sensitive information
- Security in communication between servers on the same network and with external clients

WHAT WE DIDN'T IMPLEMENT

- Check signatures
- Possibility of having more than one owner

TÉCNICO LISBOA