Petrol rationing smartcard project

Design document

Alvin Cai - s4404114
Romanos Dodopoulos - s4415191
Alexandru Geana - s4420438

1 Introduction

2 Use Case

The ration card is personalised in the backend before it is issued to the user. Users charge their ration cards at charging terminals to increase the petrol balance in their card. Petrol pumps are equipped with card terminals and will only supply petrol upon presentation of a valid ration card with sufficient petrol balance.

2.1 Card Personalisation and Issue

1. Car owners apply to the government for personalised ration cards.
2. The government verifies that the applicant does not currently have an active card and generates a personalised card loaded with:
   - PKI certificate identifying the car owner, signed by the Intermediate Cards Certificate Authority (CA).
   - The corresponding private key
   - Intermediate Pump CA and Intermediate Charging CA
   - Randomly generated secret PIN.
3. The card and secret PIN are delivered to the car owner through a secure physical channel. For instance, self-collection from municipal hall together with identity checks.

2.2 Withdraw Petrol and Charge Card

Authentication Phase Petrol terminals and rationing terminals contain a PKI certificate identifying the terminal, signed by an Intermediate CA. Each terminal also stores its private key and all of the Intermediate CAs.

These certificates are used by the smartcard and petrol terminal to mutually authenticate each other and establish an encrypted and authenticated connection. Thereafter, the card owner enters his secret PIN into the terminal. A maximum of three consecutive wrong attempts are allowed before the card is disabled.

If the PIN is correct, then the user can proceed to the petrol withdrawal or charging phase, depending on which terminal he is at.

Petrol Withdrawal Phase Personalisation and Issue

1. The card owner send to the terminal its current balance. The balance is signed by the terminal with which it had completed its previous transaction.
2. The card owner inputs the amount of petrol he would like to withdraw into the terminal.
3. The petrol pump terminal allows the transaction if and only if the following conditions are satisfied:
   - The amount is less than or equal to the available petrol ration on the card.
   - The total amount withdrawn since the last update in a charging terminal is less than or equal to 250 liters (125
   - The total transactions since the last update in a charging terminal are no more than 5 (log capacity).
4. The pump then atomically reduces the requested amount on the card.
5. The fuel is released.
6. If the tank cannot fit all the prepaid fuel, the terminal asks for a new signature for the actual amount and the balance on the card is updated again.
7. The card is released.

Charging Phase

1. Charging terminals are connected to a backend database which maintains records of each car owner and their available petrol ration.
2. If the card hasn't been charged already that month, the charging terminal increases the petrol ration in the card by the fixed monthly allowance (200 liters) and updates the backend database.
3. If a car owner did not charge the card for the previous month, it does not carry over to the current month, but is forfeit.

Decomissioned Card

1. Cards may be decomissioned when they are lost, or are expired.
2. Lost cards are reported to the government agency.
3. The status of these cards are updated as revoked in the government CA database.
4. ...

3 Security Requirements

4 Design

4.1 Certificates

4.2 Mutual Authentication and Secure Channel

4.3 Petrol Pump and Charging Terminal