Hardware Security: JavaCard

Design document - petrol allowance

Radboud University Nijmegen

Group 2: Wouter Kuhnen (s4081420), Wouter van Kranenburg (s4319176), Ye Myat Kaung (s4460677), Stephanie Silvius (s4380479)

May 31, 2016

Contents

1 Terminology and abbreviations

The following terminology and abbreviations will be used throughout this document.

PRS	Petrol Rationing System
IT	Personalisation terminal, used for the initialisation of the petrol card
PT	Petrol terminal
CT	Charging terminal
For the protocols:	
$ENC_{SK}\{X\}$	encryption function for X with symmetric key (SK) agreed to by both parties
$SIG[X]_{priv}$	signing function for X with private key of sender
$[X]_{pub}$	encryption function for X with a public key of the sender
$certificate_X$	certificate of X
pub_X	public key of X
$priv_X$	private key of X
ID_X	Identification (ID) number of X
SK	Symmetric Key
$Verify(cert)$	Certificate Verification function
$Log()$	Logging function to keep track of transactions
T	Terminal (charging/petrol)
PC	Petrol Card
BE	Back-end
VTS	Valid timestamp until certificates are considered untrusted (24Hours from the time the CVR was requested)
TS	Timestamp
$Certs$	List of certificates that are valid and or revoked
CVR	Certificate Validity Request function
PIN	PIN number
PIN_{AUTH}	Boolean response to indicate validity of PIN
$Calc()$	Petrol points calculation function based on current balance & pumped amount (in liters)
B	current petrol balance (in liters)
UB	used up petrol balance (in liters)

2 Introduction

This document describes the design decisions and security requirements for the Petrol Rationing System (PRS) that was created for the course Hardware Security at the Radboud University Nijmegen.

3 Use cases

The PRS has five use cases which describes the life-cycle from initialisation to revocation of a petrol card. Figure 1 depicts the PRS life-cycle.

- Personalisation of the petrol card with the issuer terminal (IT):
  During the personalisation phase the petrol card will be initialised with key material, a card identification number (both provided by back-end) and the current petrol balance will be set to zero.
- Charging the petrol card at the charging terminal (CT):
  The charging terminal will receive a monthly update for the petrol allowance from the back-end, which determines the amount of petrol that will be written to all petrol cards. For each presented petrol card a validation is needed if the petrol card is still valid, afterwards the card owner can charge the full monthly petrol allowance to his petrol card balance. Sub-charges of the petrol allowance are not possible. The updated balance will be immediately available for use.
- Getting petrol at the petrol terminal (PT):
  At the petrol terminal the card owner presents his petrol card. The card owner is able to see his current petrol allowance, after choosing the type of petrol and the amount of petrol he wishes to buy, the PT will remove the chosen petrol balance from the petrol card.
- End-of-life:
  Once a card reaches end-of-life (EOL), it has to be blocked and possibly decommissioned. After 5 years petrol cards will automatically be blocked.
- Stolen Card:
  If a card is stolen or lost, all key material and certificates needs to be revoked. All petrol and charging terminals will receive an updated revocation list during the night.

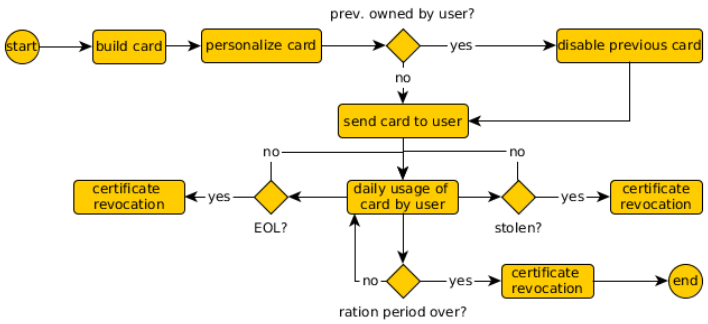

Figure 1: The life-cycle of a petrol card in the PRS.

4 Assets

Our project case involves the following assets. Items enlisted with a * have not been implemented in the PRS due to time constraints and/or technical problems.

- Petrol
- Petrol card
  - Card certificate, created with its own public and private keypair
  - *Certificate from CA
  - *Signed timestamp of last requested revocation list received from CA
  - *Timestamp indicating last charge
  - Current balance on the petrol card
  - PIN code
- Personalization terminals
  - *Terminal certificate, created with its own public and private keypair
  - Certificate from CA
  - Terminal identification number
- Charging terminals
  - *Terminal certificate, created with its own public and private keypair
  - Certificate from CA
  - *Signed timestamp of last requested revocation list received from CA
  - Current monthly allowance that will be provided to all charging terminals
  - List of revoked certificates
- Petrol terminals
  - Terminal certificate, created with its own public and private keypair
  - Certificate from CA
  - *Signed timestamp of last requested revocation list received from CA
  - List of revoked certificates
- Back-end
  - Backend certificate, created with its own public and private key
  - Current monthly allowance that will be provided to all charging terminals
  - List of all generated certificates for terminals and petrol cards

- List of revoked certificates
- *The back-end will have a sub-CA certificate
- *The main CA certificate will only be used to sign and revoke sub-CA certificates

5 Stakeholders

The PRS has different stakeholders. The government is involved for the purpose of regulating the fuel consumption of the inhabitants. Petrol companies are involved for providing the fuel and for modifying their pumping installations to accommodate the PRS. They typically want low cost and low interaction/maintenance systems. The last stakeholder would be car owners, these are the end-users of the PRS and the owner of the petrol card. They typically want easy-to-use systems and a certain degree of privacy.

6 Assumptions

During the design of the PRS assumptions are made, these are listed below.

- Petrol card:
  Every car owner will only have one petrol card. The petrol card is tamper-resistant, and therefore provides integrity and confidentiality to the data and functionality on the card, such as key material. Upon presenting a card to a terminal, the balance on the petrol card can only be modified by an authenticated charging terminal. Petrol cards will automatically expire and revoked after 5 years.

- Terminal: all terminals have a reliable clock. The key material and program code on the terminal cannot be copied or modified. The terminals are pre-installed at a secure location by screened personnel.

- Personalization:
  The code created for the PRS has been written by screened personnel and verified by various knowledgeable people whom have not detected backdoors in the code.

- Charging:
  The charging terminal will verify that the petrol balance is only increased once a month.

- Pumping:
  The pump is trusted to always communicate the right amount of fuel that has been released to the pumping terminal. The pumping terminal is able to store logs of transactions without compromising the integrity or confidentiality of the logs.

- Back-end:
  The key material of the CA cannot be copied. The revocation list maintained by the back end cannot be altered in such a way that already revoked petrol cards or terminal will be removed from the revocation list.

7 Attacker model

At any point in time it is likely that an attacker will try to perform an attack on the PRS. Likely adversaries for the PRS are: (organised) criminals, insiders and researchers. While most of the adversaries' capabilities, intentions and skills are alike, some may vary. Organised criminals are most likely to make money e.g. by obtaining and selling more petrol than rationed (or without collecting rations) and by obtaining legitimately issued petrol cards. To reach their goal they are more likely to take actions as extortion and violence. This group usually has the availability of large amounts of money to accomplish their goals.

Insiders have access or knowledge on the PRS and are familiar with the weak spots of the system. They will know or find ways to use this to their advantage. This group may try to bring down, or sabotage the workings of the system for a larger group of users. Attacks made by this group are likely to be accomplished with limited resources or money.

Researchers are sometimes provided with full specifications on a system and protocols. They are likely to break protocols such that they can intercept and manipulate any traffic between the petrol card and a terminal. This group will typically include researchers at an university, or a company hired to test the security of the system. The goals will be to break the security of the PRS in any way, which sometimes can result in a publication. This group usually has limited time and/or resources to accomplish their goals.
Attacks by these adversaries can include, but are not limited to, MiTM, card tears and compromisation of key material. In case key material of a petrol card is compromised it should not bring down the PRS. An adversary will not be able to tamper with the petrol cards, nor will they be able to build a backdoor in the software of the terminals.

8 Security requirements

1. Confidentiality
   (a) The certificate and key material shall only be revealed to the IT/CT/PT after the terminal has been authenticated.
   (b) The card usage shall not be revealed to any kind of terminal.
   (c) The PIN code shall only be know by the petrol card and the petrol card owner.

2. Integrity

   (a) The petrol balance on the petrol card can only be altered by an authenticated terminal.

   (b) The identity number of the petrol card cannot be altered.

   (c) The certificate and key material on the petrol card and terminals cannot be altered.

   (d) The logs on the terminal can only be altered by the terminal itself.

   (e) Communication between the terminals and back-end will be secure after they have both authenticated towards each other.

3. Authentication

   (a) The card owner shall authenticate to the CT or PT by entering the PIN to the petrol card.

   (b) The back end will only provide the monthly allowance to the CT after it has authenticated itself.

   (c) Communication between the terminals and back-end will be secure after they have both authenticated towards each other.

4. Authorisation

   (a) The CT is only authorised to update the petrol allowance to the petrol card once every month.

   (b) The PT is authorised to withdraw petrol balance from the petrol card during a petrol transaction.

5. Non-repudiation

   (a) The CT can prove to the back-end that it charged the monthly allowance to a valid petrol card.

   (b) The PT can prove to the back-end that it collected petrol allowance from a valid petrol card.

9 Design decisions

During the design of the project, several design decisions were made, they are listed here.

- Petrol cards
  - PIN code is used for authenticating the card owner to the terminals.
  - Public Key Infrastructure (PKI) is used for authentication, encryption and signatures of messages.
  - The petrol card will have an initial balance of zero once a car owner receives the petrol card.

  - A symmetric key is used to secure communication between the petrol card and the terminal.
  - Petrol cards will have their own certificates and key material that will be initialised by the IT.

- Terminal
  - The IT will set the initial balance to zero.
  - The PIN codes will be set by the IT.
  - The CT will relay the signed allowance by the back end to the petrol card.
  - A symmetric key is used to secure communication between the terminal and back-end.
  - The petrol allowance on the petrol card can only be charged once a month.
  - The CT can see the petrol balance stored on the petrol card after the CT has authenticated itself to the petrol card.
  - The card owner will have to specify the required amount of petrol that he wishes to pump at the PT. In a previous design we planned on subtracting all balance from the petrol card.

- Back-end
  - The back-end will sign and send the latest version of the CRL to the terminals

9.1 PIN codes

The user will have to enter a PIN code on the terminal numpad to verify ownership of the petrol card to the terminal. The terminal will send the PIN signed by its private key with the plain text of the PIN to the petrol card through the mutually authenticated encrypted channel. By which the petrol card will reply with whether the PIN number is correct or not.

9.2 Cryptography and PKI

PKI is used to maintain and generate certificates. The back-end will operate as CA. We planned on creating a sub-CA to sign all terminal and petrol card certificates, but due to time constraints this was not possible. In the current situation the certificate of the main CA will be stored on a newly personalised petrol card. The back-end, terminals and petrol cards will all have a RSA-1024 bit keypair. While this is not secure for real-world purposes, for testing and petrol card limitations, this will have to do. The petrol card and terminals will receive a timestamp of the last update of certificate revocation list which is signed by the main CA certificate. This way it can be verified if the provided

revocation list is recent. Each terminal will have the same setup: main CA certificate, its RSA keypair, and signed timestamp of the last updated certificate revocation list.

The CA certificate on each device is used to verify the validity and authenticity of each certificate during communication. Each end point, i.e petrol card and terminal, will verify the certificate of the other end point it is connecting to. In case the CA is notified of abuse or a breach, the certificate belonging to the end point will only be usable for 24 hours until the revocation list has been pushed to the end points.
Public and private keys in each end point will be used in conjunction with the CA certificate to mutually authenticate between each other. It is also used to negotiate a SK and also to provide integrity of the message by signing them.

9.3 Protocol Descriptions

9.3.1 Mutual Authentication

First the terminal sends a command APDU to enable the correct applet from the petrol card for the petrol rationing system. After that the terminal sends its certificate and public key to the petrol card. The petrol card verifies the certificate of the terminal and chooses a SK for encrypted communication. The petrol card signs its identification number with its private key, encrypts that signature and its own certificate with the SK. Then it sends the encrypted signature and certificate together with the SK encrypted by the public key of the terminal. Once the terminal receives the certificate of the petrol card, it verifies it. It then signs its own signature with its private key and combines this with a signed version of the identification number, encrypts them both with the SK and sends it to the petrol card.

$$
\begin{aligned}
T \rightarrow PC &: \text{commandAPDU to enable applet.} \\
T \rightarrow PC &: certificate_T, pub_T \\
PC &: \text{Verify}(certificate_T)\text{and choose SK} \\
PC \rightarrow T &: ENC_{SK}\{SIG[ID_{PC}]_{priv_{PC}}, certificate_{PC}\}, [SK]_{pub_T} \\
T &: \text{Verify}(certificate_{PC}) \\
T \rightarrow PC &: ENC_{SK}\{SIG[ID_T]_{priv_T}, ID_T\}
\end{aligned}
$$

and now we have a encrypted channel between a terminal and a petrol card.

9.3.2 Certificate Validity Request

After mutual authentication has been done, the petrol card will request the certificate revocation list from the terminal, who already has access the latest revocation list from the back-end. The revocation list is signed by the back-end.

$$PC \rightarrow T : [CVR + pub_{PC}]_{pub_{BE}}$$
$$T \rightarrow PC : [SIG[VTS, TS, Certs]_{priv_{BE}}, VTS, TS, Certs]_{pub_{PC}}$$

9.3.3 PIN validation and authentication of card owner

After mutual authentication has been done, the terminal receives a PIN on the numpad from the card owner, signs the PIN and send the encryption of the signature with the plaintext PIN number to the petrol card. Once the petrol card receives the PIN number, returns the encrypted and signed boolean value (True/False) to the terminal after it verifies the PIN number.

PIN validation and authentication of card owner guarantees security requirement 1(d).

$$T \rightarrow PC : ENC_{SK}\{SIG[PIN]_{priv_T}, PIN\}$$
$$PC \rightarrow T : ENC_{SK}\{SIG[PIN_{AUTH}]_{priv_{PC}}, PIN_{AUTH}\}$$

9.3.4 Getting petrol from the petrol terminal

After mutual authentication and authentication of the card owner, the petrol card can send its current balance to the petrol terminal for getting petrol. The card owner will have to specify the amount of petrol he wishes to subtract from his balance. The PT will verify if this is possible and subtract this amount from the petrol card. After the transaction has been verified the PT will write a log entry with the time, identification number of the petrol card, balance and amount of petrol that was pumped. If a card tear occurs the specified amount of petrol will be reduced from the petrol cards balance. We planned on adding something to this log that is signed by the card (such as balance and/or timestamp), however due to time constraints this was not implemented.
The terminal logging the timestamp, identification number and the balance before the petrol being pumped guarantees security requirement 5(b).

$$\begin{aligned}
PC \rightarrow T &: ENC_{SK}\{SIG[B]_{priv_{PC}}, B\} \\
T &: \text{Log}(TS, ID_{PC}, B, SIG[TS, ID_{PC}, B]_{priv_T}) \\
T \rightarrow PC &: ENC_{SK}\{SIG[BZ]_{priv_T}, BZ\} \\
T &: \text{Calc}(B = B - UB) \\
T \rightarrow PC &: ENC_{SK}\{SIG[B]_{priv_T}, B\} \\
T &: \text{Log}(TS, ID_{PC}, B, UB, SIG[TS, ID_{PC}, B, UB]_{priv_T})
\end{aligned}$$

9.3.5 Charging petrol allowance to the petrol card

After mutual authentication, PIN validation and authentication of card owner has been done, the petrol card can ask the charging terminal to charge its

allowed monthly petrol balance. Then the terminal starts a mutually authenticated encrypted channel between itself and the back-end to get the monthly petrol allowance, and then writes those values back to the petrol card.

The terminal starting a mutually authenticated encrypted channel with the back-end to get the monthly petrol allowance guarantees security requirement 1(e) & 3(c).

The terminal logging the timestamp, identity number and the balance being written to the petrol card guarantees security requirement 6(a).

$PC \rightarrow T$: request APDU to initiate charging monthly allowance

T : requests monthly allowance from back-end through the encrypted channel

T : Log$(TS, ID_{PC}, B, SIG[TS, ID_{PC}, B]_{priv_T})$

$T \rightarrow PC : ENC_{SK}\{SIG[B, TS]_{priv_{BE}}, B, TS\}$

9.3.6 Invalidating petrol cards

Petrol cards are invalidated by the back-end by means of revoking the certificate, which will be added to the revocation list. Cards can be added to the revocation list if the certificate is valid, if authentication of the user failed (incorrect PIN entry for three times), or any other suspicious behaviour Possible other scenarios...
TODO: explain how persistant and transient states are realised in the code

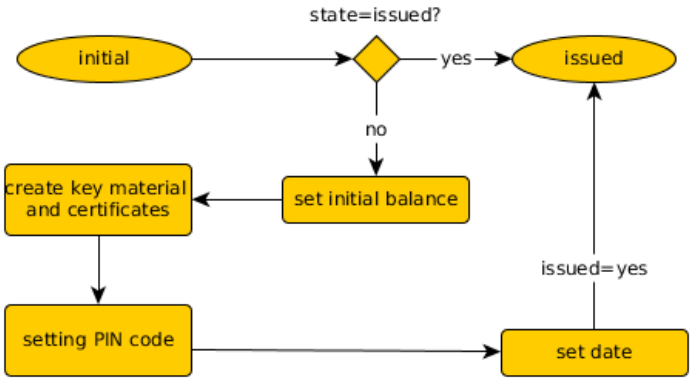

Figure 2: The persistant states of the petrol card.

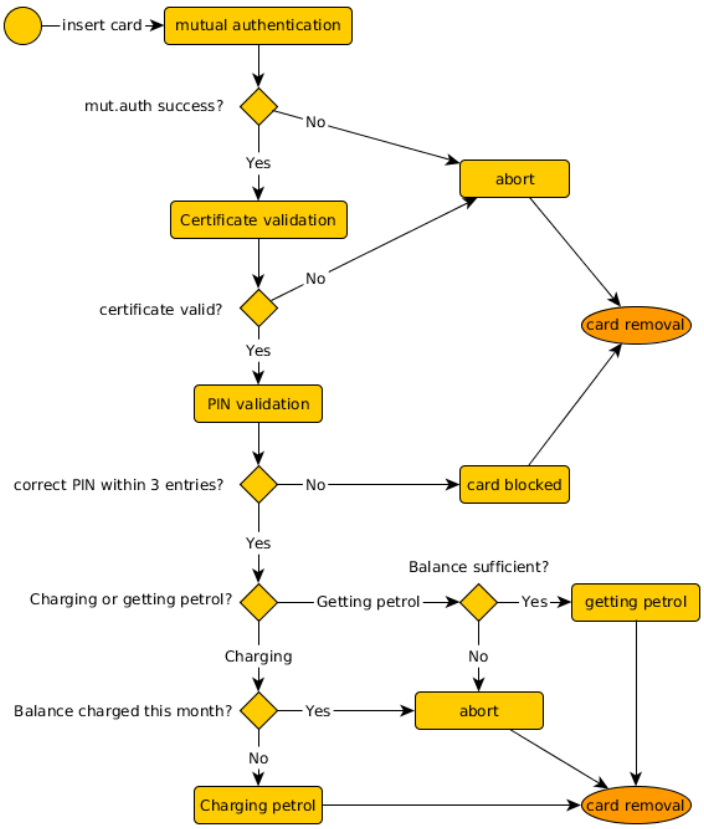

Figure 3: The transient states of the petrol card.