C-ROADS

SCOOP@F PKI TECHNICAL SPECIFICATIONS

IDnomic

22/03/2017

Co-financed by the European Union
Connecting Europe Facility

Outline

1. SCOOP@F PKI Presentation
2. SCOOP@F PKI Architecture
3. SCOOP@F PKI Components
4. SCOOP@F PKI use cases

Co-financed by the European Union
Connecting Europe Facility

1.SCOOP@F PKI Presentation

PKI design :

- Compliant with ETSI standards (TS 103 097, TS 102 941)

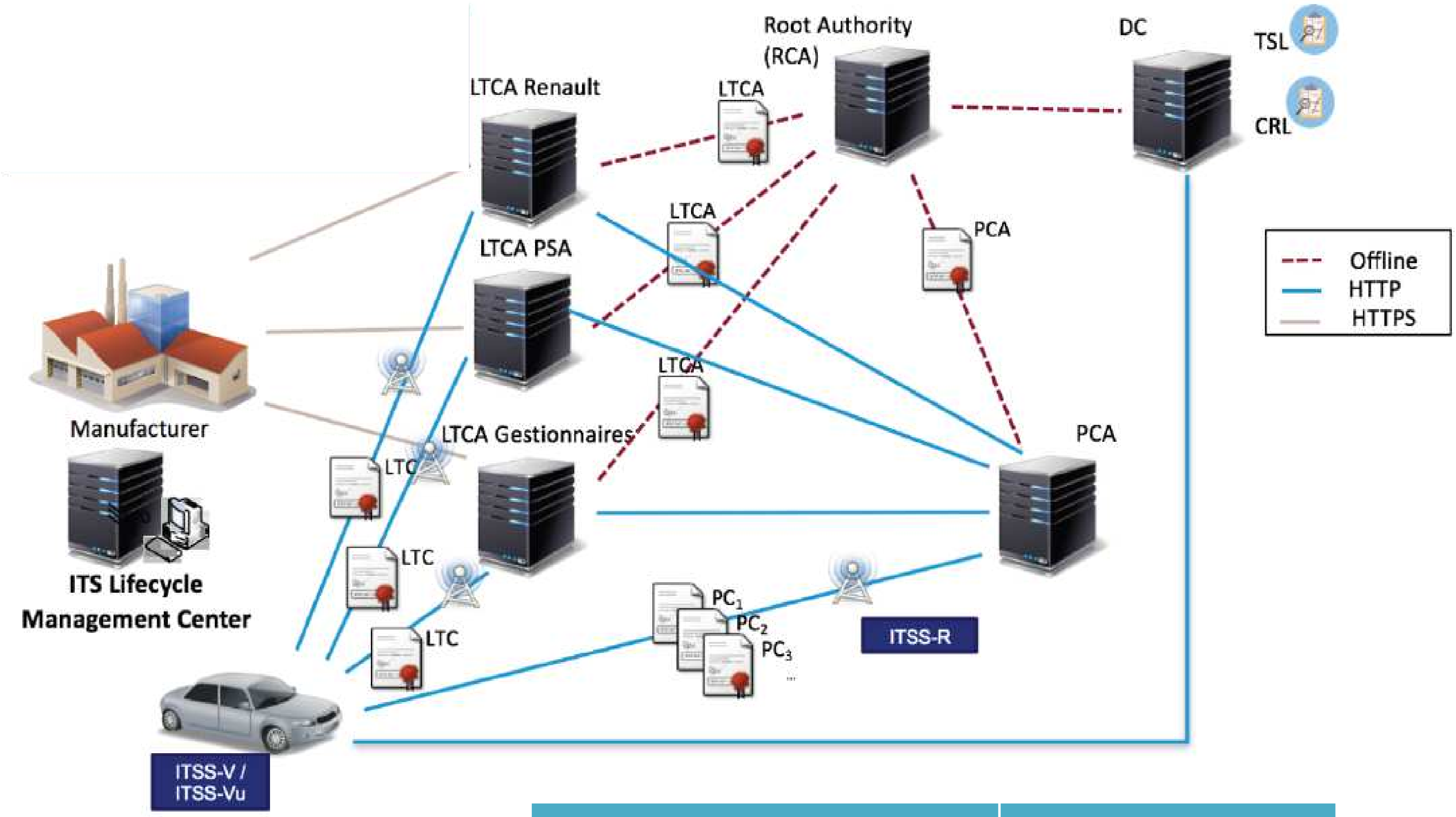
PKI based security solution covers:

- ”**Integrity",** with message signature
- **”Privacy",** thanks to the separation between LTCA and PCA, and use of pseudonyms
- **”Non-repudiation"**
- **”Authentication"**

But does not support:

- **”Confidentiality",** CAM and DENM messages are not encrypted
- **“Plausibility and Availability”**

2.SCOOP@F PKI Architecture



SCOOP@F PKI	ITS ETSI Standards
Long Term Certificate Authority (LTCA)	Enrolment Authority (EA)
Pseudonym Certificate Authority (PCA)	Authorization Authority (AA)
Long Term Certificate (LTC)	Enrolment certificate (EC)
Pseudonym Certificate (PC)	Authorization Ticket (AT)

Co-financed by the European Union
Connecting Europe Facility

3.SCOOP@F PKI Components

- **Root Certificate Authority (RCA):** is the root of trust for all certificates within the PKI hierarchy. It operates in an offline mode and is responsible for the management of LTCAs and PCAs (creation, security requirements authorizing the issuance of certificates to ITSSs).

- **Long Term Certificate Authority (LTCA):** is a security management entity responsible for the issuance of LTC and the validation of PCs as well as the management of the ITSSs (registration, status update, permissions…). It operates in an online mode.

- **Pseudonym Certificate Authority (PCA):** is a security management entity responsible for the delivery, the monitoring and the use of PCs. It operates in an online mode.

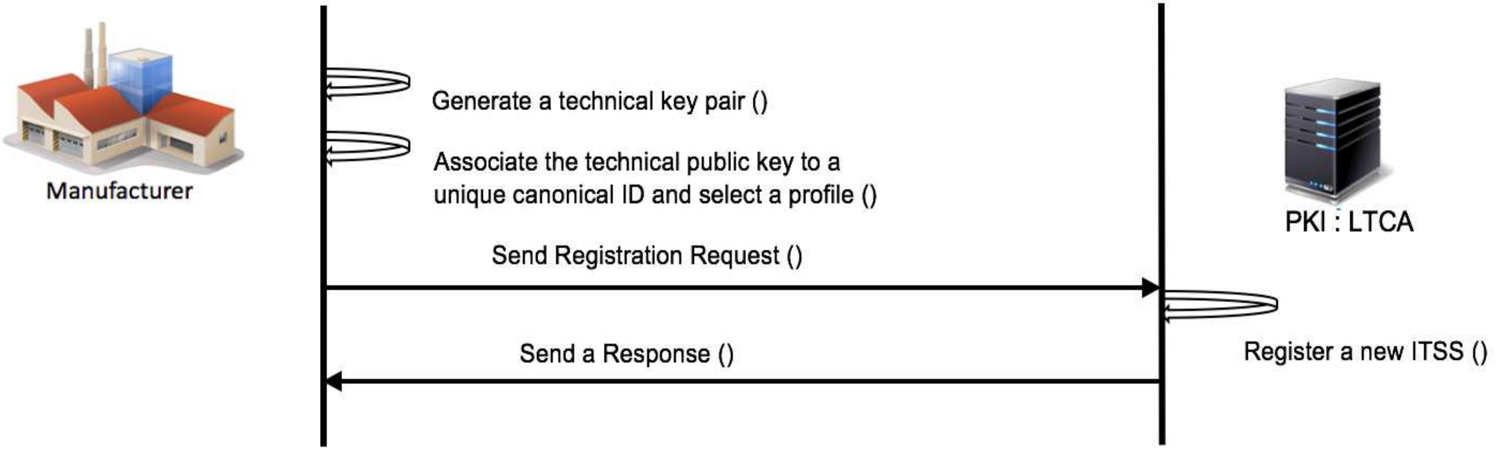
- **Distribution Centre (DC):** provides the ITSSs with the updated trust information such as TSL and CRL necessary to assure that received information is coming from legitimate and authorized ITSSs or PKI certification authority.

3.SCOOP@F PKI Components

- **ITSS:** ITS station (vehicle, RSU)
- **Long Term Certificate (LTC):** gives its holder (ITSSs) the right to request PCs.
- **Pseudonym Certificate (PC):** gives its holder (ITSSs) the right to perform specific actions.
- **Certificate Revocation List (CRL):** is a list digitally signed by a CA that contains certificates identities that are no longer valid.
- **Trusted Services List (TSL):** is a signed list which contains trusted RCAs, LTCAs and PCAs certificates and PKI service access points. This list is updated frequently.

4.SCOOP@F PKI Use Cases

ITSS Registration

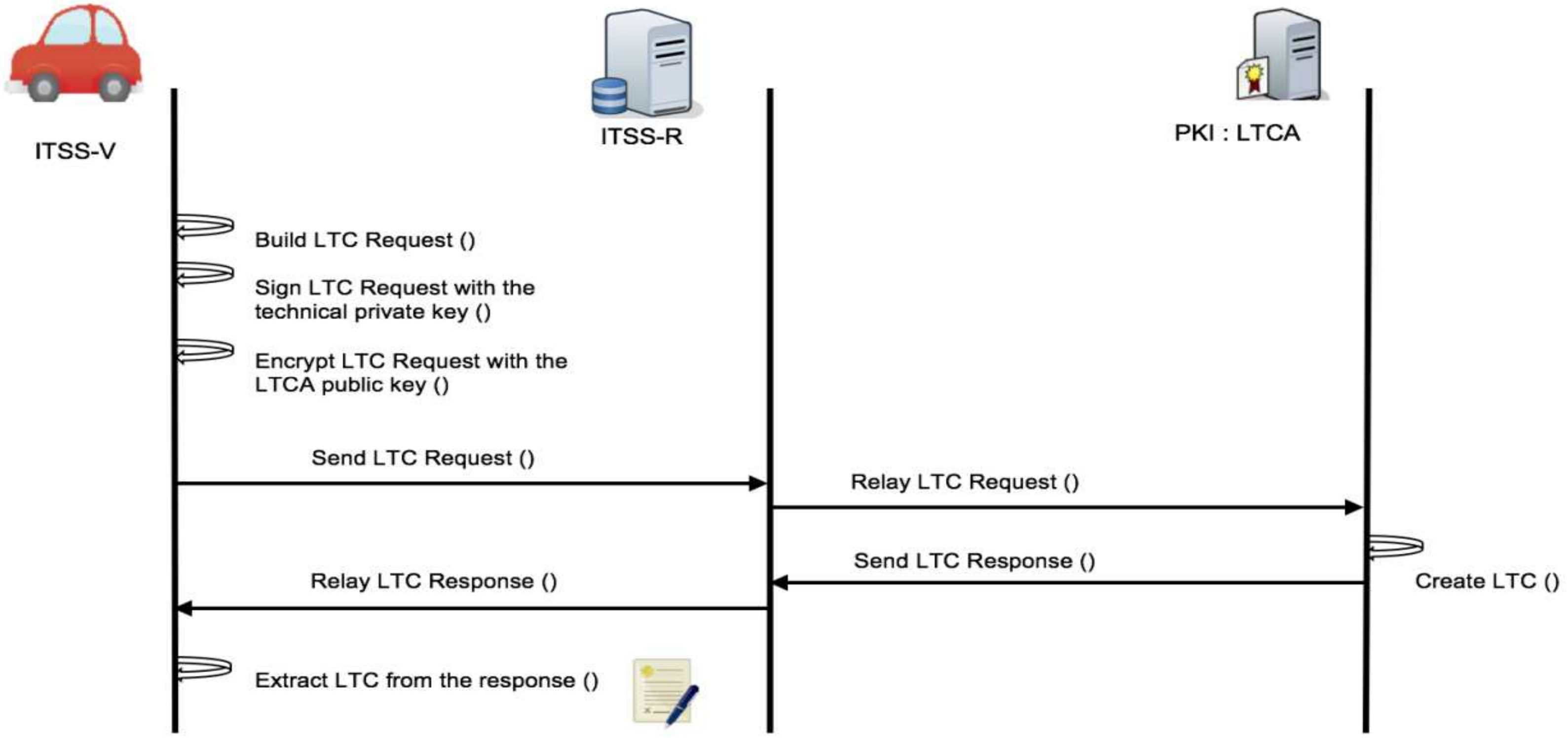

Manufacturer
Generate a technical key pair ()
Associate the technical public key to a unique canonical ID and select a profile ()
Send Registration Request ()
Send a Response ()
PKI : LTCA
Register a new ITSS ()

- The manufacturer registers its ITSSs in the PKI via the operator interface (HMI, Web Service).
- Authentication using X509 certificate is required.
- The registration of ITSSs by batch is possible via .csv file.

Co-financed by the European Union
Connecting Europe Facility

4.SCOOP@F PKI Use Cases

LTC Request

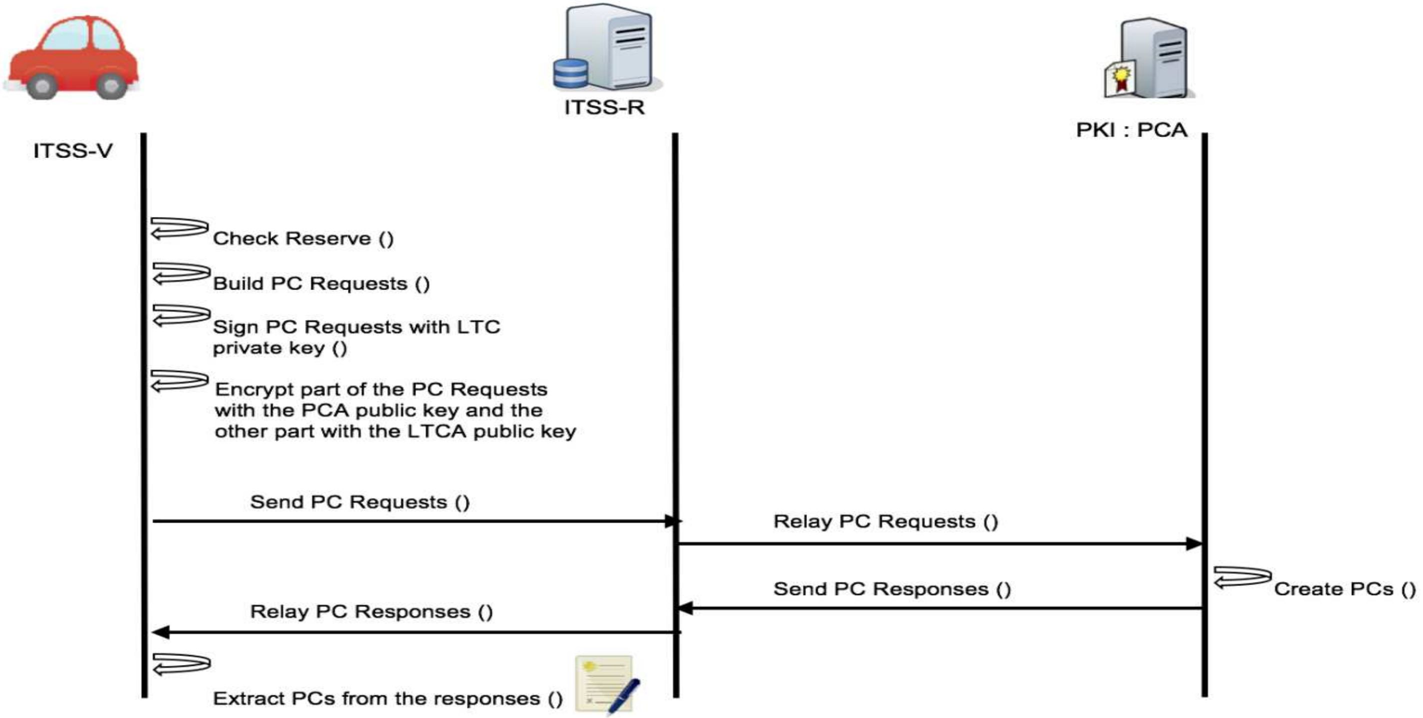


- The ITSS-R and road managers' ITSSs communicate straight with LTCA without relay.
- The LTC's format is described in the ETSI TS 103097 v1.2.1

Co-financed by the European Union
Connecting Europe Facility

4.SCOOP@F PKI Use Cases

PC Request

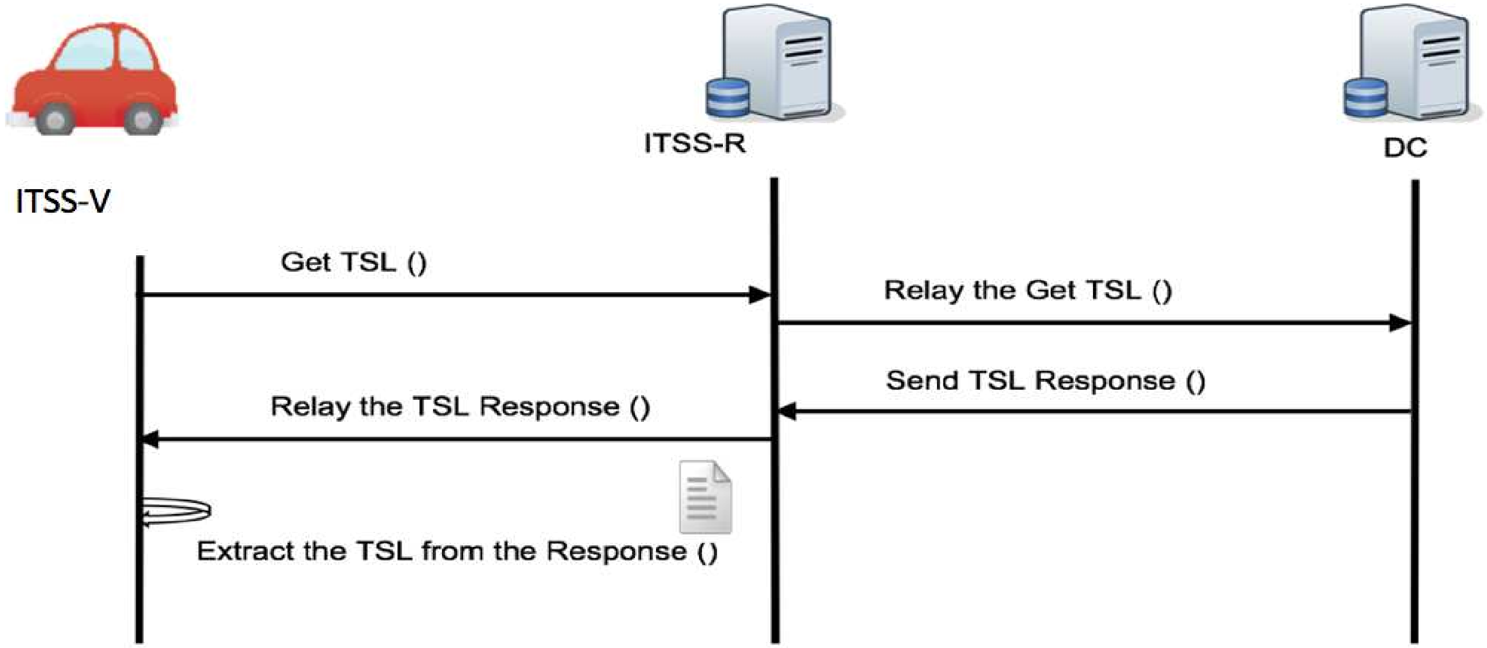

ITSS-V
ITSS-R
PKI : PCA
Check Reserve ()
Build PC Requests ()
Sign PC Requests with LTC private key ()
Encrypt part of the PC Requests with the PCA public key and the other part with the LTCA public key
Send PC Requests ()
Relay PC Requests ()
Create PCs ()
Send PC Responses ()
Relay PC Responses ()
Extract PCs from the responses ()

- The ITSS-R and road managers' ITSSs communicate straight with LTCA without relay.
- The request of pool of n PCs is possible by sending n requests.
- The PC's format is described in the ETSI TS 103 097 v1.2.1

Co-financed by the European Union
Connecting Europe Facility

4.SCOOP@F PKI Use Cases

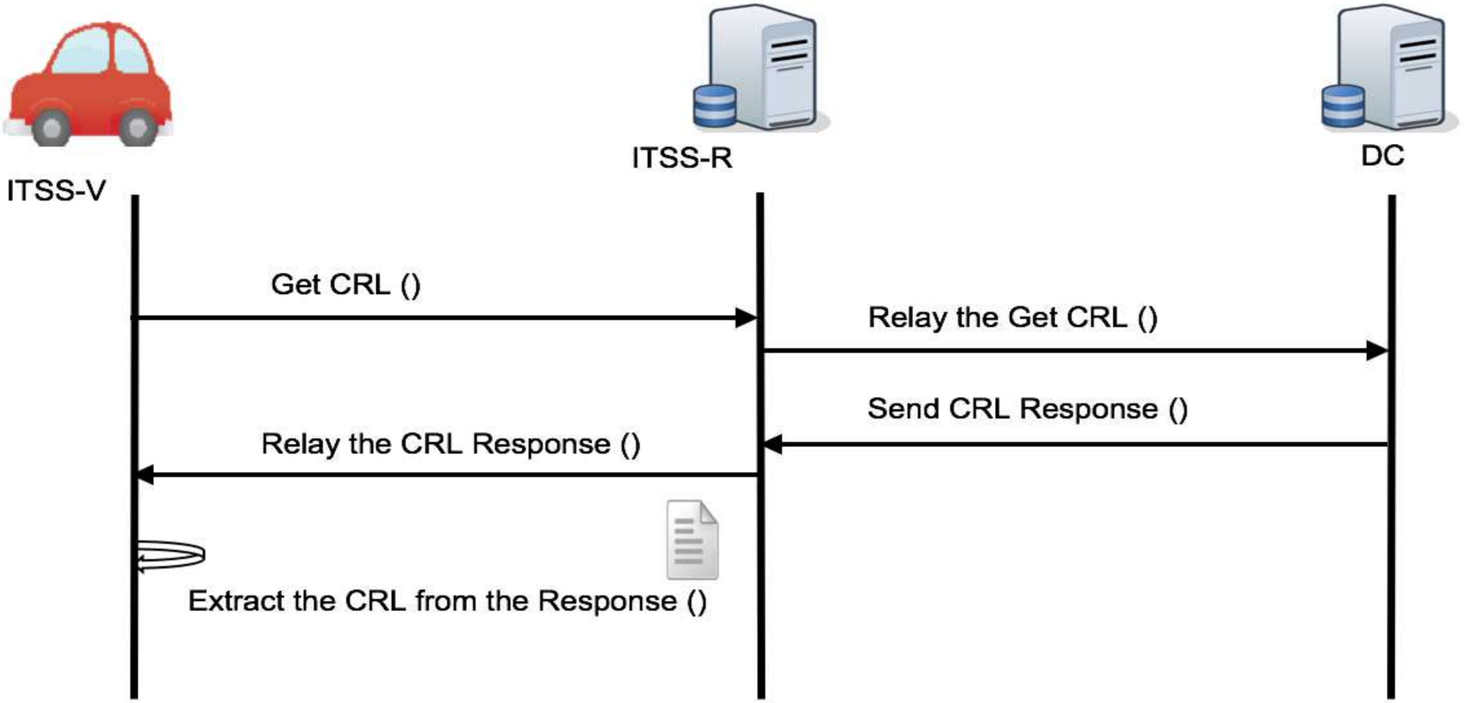
TSL Download



- Upon the download of TSL, the ITSS must verify that it is signed by the RCA.

4.SCOOP@F PKI Use Cases

CRL Download



- Upon the download of CRL, the ITSS must verify that it is signed by the RCA.

C-ROADS

THANK YOU!

Co-financed by the European Union
Connecting Europe Facility