escrypt
Embedded Security by ETAS

ETSI Plugtest C2C-CC PKI User Guide

Table of Contents

1 Introduction

Note: The Pilot PKI is an infrastructure that is to be used for testing purposes in development processes. Usage of the PKI will be tracked. The operators of the PKI reserve their right to restrict or deny access to the PKI in case of misuse.

1.1 Contents

The Pilot PKI contains different documents:

- This documentation
- C2C-CC Specification of message formats for PKI communication [RD-1]

1.2 Overview

The Pilot PKI comprises the management of the certification authorities of the infrastructure side, which consists at minimum of three different CAs following different roles. The Pilot PKI includes one Root CA (RCA), as shown in Figure 1. This RCA manages the root certificate and issues the Enrollment Authority (EA) and the Authorization Authority (AA) on top of the PKI hierarchy.

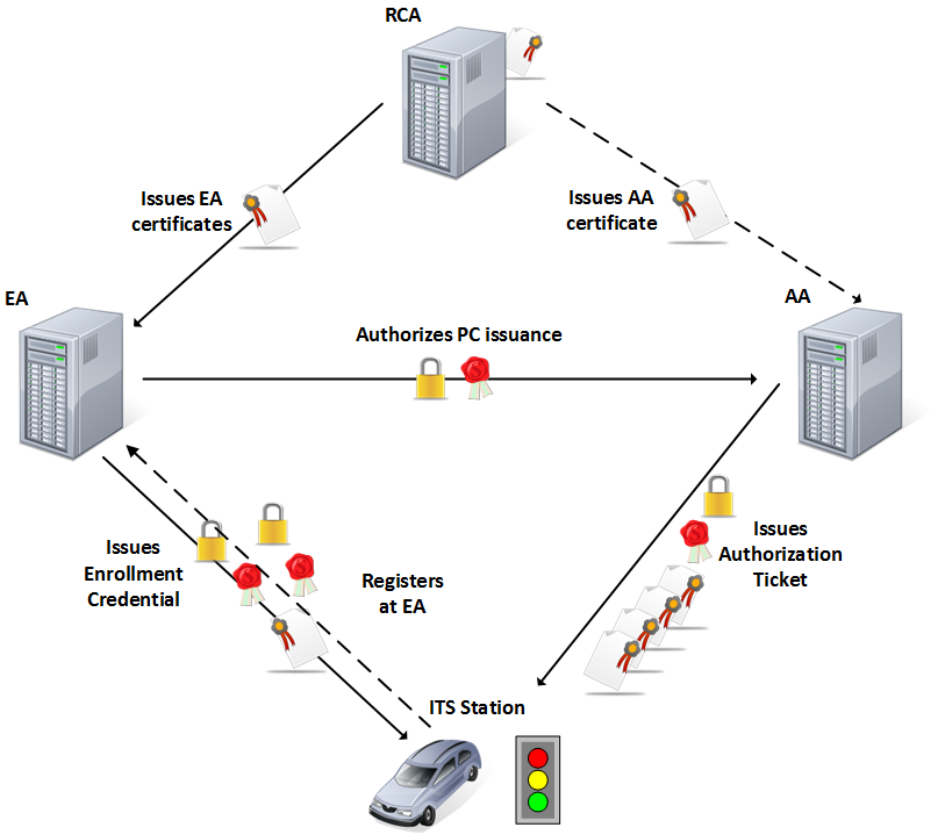

Figure 1 PKI hierarchy

The RCA is the trust anchor in the PKI issuing certificates for EAs and AAs. The PKI is designed to be limited to these two layers. An EA or an AA is not permitted to issue additional intermediate CAs. The EA is responsible to manage registered ITS stations and issues long-term certificates, called Enrollment Credential (EC) that are used to request Authorization Tickets (AT). The ITS station requests the EC from the EA and ATs from the AA.

2 The Pilot PKI's components

The three different CAs included in the Pilot PKI, described in the following, are all operated by ESCRYPT GmbH – Embedded Security.

The PKI provides the following web services, which are available by the following URLs:

- RCA web service: https://22.test.mcg.escrypt.com/V2XWebService/RcaMcgWebService
- EA web service: https://22.test.mcg.escrypt.com/V2XWebService/EaMcgWebService
- AA web service: https://22.test.mcg.escrypt.com/V2XWebService/AaMcgWebService

2.1 RCA

The RCA certificate can be downloaded via the MCG interface of the RCA web services.

2.2 Enrollment Authority (EA)

The MCG interface of the EA web service provides the following services for the EA:

- Download of EA certificate
- Request and Acknowledgement of Enrollment Credentials

2.2.1 Registration of ITS station

For the ETSI Plugtest the registration of ITS stations is performed by ESCRYPT. Therefore, all ITS station owners are requested to send an e-mail providing the following information:

- 16-byte module id: This id is the unique canonical identifier identifying the ITS station's security module. The module id must have a length of 16 byte and should be provided as a HEX string. For the 8 most significant bytes, a fixed ID block like the first 8 characters of the company name could be used (e.g. ESCRYPT = 4553435259505400), whereas the remaining 8 byte count up the ITS stations.
- Module authentication key: The ITS station's security module contains a randomly generated ECC NIST P-256 key pair. The public key must be transferred to the EA during the registration process. The corresponding private key is later used to sign the request for a long-term certificate.
- Assurance Level: See ETSI TS 103 097 for explanation.
- List of AID/SSPs: See ETSI TS 103 097 for explanation. Our PKI supports the following AIDs:
  - 36 CAM
  - 37 DENM
  - 137 SPAT messages
  - 138 MAP messages

- 139 IVI messages
- 140 SRM/SSM (Traffic Light Control Service – TLC)
- 141 GN-MGMT

2.2.2 Requesting enrollment credentials

- Enrollment credentials (ECs) can be requested using the appropriate web service method with request message of type **`LtcRequest`** of the Security Management Formats document.
- The request message must be signed using the ITS-station's private key which matches the public key from the registration**.**
- The parameters of the request message shall be filled with those values that the requester wants to be written in the EC certificate. When the EA certificate specifies AIDs, the EC request must contain a valid AID and SSP.

2.3 Authorization Authority (AA)

In addition to the services listed above, the AA web service also allows to download the AA certificate, as well as requesting authorization tickets (AT).

2.3.1 Requesting authorization tickets

- Authorization tickets (ATs) can be requested using the appropriate web service method with request message of type **`PcRequest`** of the Security Management Formats document.
- For each requested certificate, an ECC NIST P-256 verification key pair must be generated.
- Optionally, encryption key pairs can be generated. The public keys must be put in the respective lists of the **`PcRequest`** message.
- The request message must be signed using the EC private key.

2.4 The parameters of the request message shall be filled with those values that the requester wants to be written in the AT certificate. When the EC certificate specifies an AID and SSP, the AT request must contain a valid AID and SSP. Specification of message formats

The message formats that are used to communicate with the PKI are specified in this document **[RD-1]**.

A1. Glossary

AA	Authorization Authority	Certificate Authority that issues authorization tickets
AT	Authorization Ticket	Short-term certificates for pseudonymous communication
C2C-CC	C2C-Communication Consortium	
CA	Certificate Authority	
EA	Enrollment Authority	Certificate Authority that issues enrollment credentials
EC	Enrollment Credential	Long-term certificate for ITS stations
HSM	Hardware Security Module	
ITS	Intelligent Transportation System	Systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means
ITS-S	ITS Station	Generic term for any ITS station such as vehicle station or roadside unit
PKI	Public Key Infrastructure	
RCA	Root Certificate Authority	
V2X	Vehicle-to-X	Vehicle-to-Vehicle or Vehicle-to-Infrastructure
WLAN	Wireless Local Area Network	

A2. Figures

A3. References

[RD-1]	Car 2 Car Communication Consortium, "Pilot PKI: Security Management Message Formats", Version 1.0, June 2013
[RD-2]	ETSI TS 103 097 v1.2.1(2015-06), Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats

A4. Document history

Version	Date	Author	Modifications
1.0	03.07.2016	ESCRYPT	First version
1.1	14.09.2016	ESCRYPT	Updated URLs for V2X PKI