8th Conference on Informatics and Information Technology with International Participation (CIIT 2011)

ARCHITECTURAL AND DESIGN OVERVIEW OF DIGITAL TACHOGRAPHS IN MACEDONIA

Pance Ribarski, Sashko Ristov
Institute of Informatics, Faculty of Natural Science, Ss. Cyril and Methodius University
Skopje, Macedonia
e-mail: {pance, sasko}@ii.edu.mk

ABSTRACT

This paper describes the architecture and the design of the digital tachograph system in Macedonia, especially MKD-CA subsystem, the subsystem for issuing digital certificates. The system accomplishes the security and functional requirements to be appropriate system for issuing the digital certificates for digital tachographs in Macedonia, as well as for other Member State Authorities.

I. INTRODUCTION

In order to improve working conditions, people safety and protection involved in driving, as well as to increase the safety level in road transport, Digital Tachograph System was introduced in European Union. The system assumes installation of the necessary equipment (tachograph) in the vehicles, for recording driving hours in road transport.

Digital Tachograph System is hierarchical. The root of the system is European Root Certificate Authority (ERCA), and there is a connection with different Member States, in order to create a coherent and protected system [2]. ERCA Requirements are to protect and certify national Member State keys and to create trust each other.

A. Background

Macedonia, as a country candidate for a member of a European Union, was identified as a Member State Authority (as Non EU Countries) on 01/03/2010. On 16/09/2010, [1] was approved. All key management status are given in [5].

B. Digital Tachograph System in Macedonia

On Fig. 1 is shown Digital Tachograph System in Macedonia as a part of Digital Tachograph System in EU. Ministry of Transport and Communication is authorized authority to issue and administer [1], in order to cover (where applicable) the following processes:

- issuing of tachograph cards, including keys and certificates;
- issuing of vehicle unit keys and certificates;
- issuing of motion sensor keys;
- management of the Member State keys.

Digital Tachograph System in Macedonia consists of these parts:

- MKD-CIA
- MKD-CP (Including MKD-DPS)
- MKD-CA

MKD-CIA is the authority for issuing the tachograph cards and is responsible for:

- Implementation of the system, products and services necessary for issuing tachograph cards;
- Maintenance the link between units for identification of the certificate and the users.

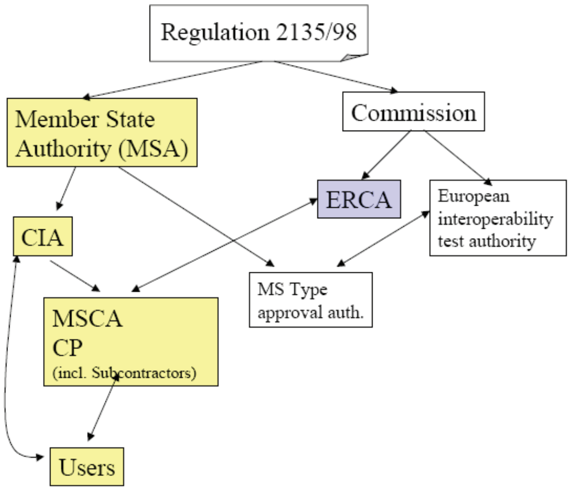
Regulation 2135/98
Member State Authority (MSA)
Commission
ERCA
European interoperability test authority
CIA
MS Type approval auth.
MSCA CP (incl. Subcontractors)
Users

Figure 1: Digital Tachograph System [6].

MKD-CP ensures that all required data are stored into digital tachograph cards, that is it personalizes the tachograph cards inside and outside.

MKD-CA is the subsystem for issuing and administering the digital certificates for the purpose of digital tachograph cards. It also generates and registers the Member State keys, and registers the ERCA root public keys. This subsystem ensures data integrity and confidentiality where needed.

C. Digital Tachograph Cards

There are four digital tachograph card types in Macedonia (Fig 2):

- Driver Card
- Workshop Card
- Control Card
- Company Card

Driver Card is issued to individuals having permanent residence in the country of application. Workshop card is issued to a workshop having valid workshop permit for Digital Tachograph. Control card is issued to a party is nominated as an official control body. Company card shall only be issued to a hauling company.

Figure 2: Digital Tachograph Cards – JRC.

II. MKD-CA Architecture

MKD-CA, as a subsystem of digital tachograph system in Macedonia is the main part for the security and trustiness of the whole system. It lies in the middle of the whole system and its main goal is to receive the certificate requests from MKD-CIA and issue the digital certificate for that request.

On Fig. 3 is shown the inside of the MKD-CA system, as well as its interfaces.

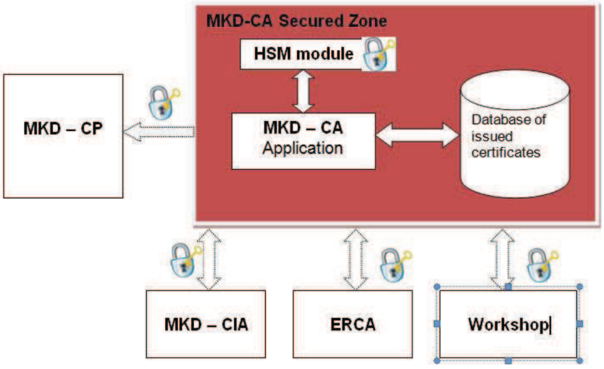

Figure 3: MKD-CA System Design and Interfaces

The whole MKD-CA system is designed in a secured stand alone zone to accomplish the security requirements given in [3] and [4]. We design the MKD-CA as a system consisted of three parts and the interfaces to connect to other Digital Tachograph System subsystems.

A. *MKD-CA Application*

This subsystem is the main part of the MKD-CA system and that is user interface to the MKD-CA operators. It receives the requests securely from MKD-CIA, issues the certificate key pair and signs the certificate with the national keys (MKD-CA root keys). Then MKD-CA Application stores the certificate into the certificate database store, and sends the sensitive information to MKD-DPS for preparation for the personalization.

B. *MKD-CA Key Store*

MKD-CA Key store, which is Hardware Security Module, creates and maintains the national keys, signs the card certificates with national keys, as well as encrypts the communication to ERCA gaining the KmWC keys. It also stores the KmWC TDES key and ERCA public root key.

C. *MKD-CA Certificate store*

The second part of the MKD-CA system is the public certificate store, which is the database, where every issued card certificates is stored. Also, this part of the MKD-CA system logs the administrators and operators activities.

D. *MKD-CA Interfaces*

We designed several interfaces on the system, and some of them are unidirectional, and others are bidirectional. Also, there are internal and external interfaces.

1) *MKD-CA – ERCA Interface*

This interface is used to send the requests for the certification of the national member state keys, from ERCA and for send the request for Motion Sensor Keys for workshops [2].

2) *ERCA - MKD-CA Interface*

This interface is used to receive the signed MKD-CA root certificate by ERCA and to receive the encrypted Motion Sensor Keys for workshops [2].

3) *MKD-CIA - MKD-CA Interface*

This interface is used to receive the requests for issuing the card certificates from MKD-CIA. There isn't direct connection between MKD-CIA and MKD-CA, because the MKD-CA isolation, but transfer between two independent physical systems.

4) *MKD-CA - Workshop Interface*

The system securely imports the KmWC Motion Sensor Key into every workshop tachograph cards through this interface.

5) *MKD-CA - MKD-CP (MKD-DPS) Interface*

This interface is used to transfer the sensitive data from the certificates to the data preparation subsystem (MKD-DPS) in order to be personalized on the digital tachograph cards.

6) *MKD-CA Application – Keystore Internal Interface*

This internal interface is the most secured part of the system. Every cryptographic operation (sign or encryption) is made through this interface.

III. MKD-CA Design

For the software part of the system we used up-to-date software platforms. We use Microsoft .NET Framework 3.5 for the MKD-CA Application with C#. For the certificate store, as well as MKD-CA administrators and operators activity logs, we use MySQL Database, secured with Database Administrator username and password. All these subsystems run on Microsoft Windows 2008 Server operating system. The communication with the HSM Module is made by the PKCS#11 standard.

IV. Conclusion

The designed digital tachograph system, especially MKD-CA, offers highly level of compatibility with other subsystems (MKD-CIA and MKD-CP). MKD-CIA interface protocol allows integrating with other Registration Authorities accomplished with the interface protocol. Interface to MKD-CP allows easy integration with particular personalization subsystem, which is particular personalization machine if having SDK.

The system offers high level reliability, because of existing test environment with test certification authority, as well as the passed certification of the MKD-CA root certificate [7] on 27/11/2010, which made the system fully appropriate as the core CA system for digital tachograph system in Macedonia.

References

[1] "MKD-MSA Policy for Digital Tachographs in Macedonia" Ministry of Transport and Communication, 2010.

[2] J. W. Bishop, J-P Nordvik, ERCA Policy V2.1. 2009.

[3] Commission Regulation (EC) No 1360/2002, Annex I(B) Appendix 11 - Common security mechanisms.

[4] FIPS PUB 140-2 Security Requirements for Cryptographic Modules NIST, 2001.

[5] "Key Management Status", http://dtc.jrc.it/key_management_status.html

[6] Guideline and Template National CA Policy for the Tachograph System, Card Issuing Project – SWG3, 2002.

[7] http://dtc.jrc.it/public_key_certificates.html