SECURITY IMPLEMENTATION OF DIGITAL TACHOGRAPH SYSTEM IN MACEDONIA

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

ABSTRACT

This paper describes the security implemented into the digital tachograph system in Macedonia, especially MKD-CA subsystem, the subsystem for issuing digital certificates, as well as the interface from MKD-CA to MKD-CP, where data integrity and confidentiality must be assured. There are some security issues that are strictly defined and mandatory, and also other security issues to be accomplished to some well known security best practice and requirements. All the required protocols are implemented in the system, as well others that assured the required level of security.

I. INTRODUCTION

In order to achieve confidentiality of the personal information, as well as data integrity, Digital Tachograph System has a part – MKD-CA for issuing and maintenance of digital certificates. [1] Describes the architectural and design overview of the whole Digital Tachograph System in Macedonia, and its parts. In this paper we describe the security overview of the developed system as required in [2], [3] and [4] where are exactly defined confidential and non confidential data, as well as mandatory security protocols for keys.

A. Key Management

The main part of the security assures the HSM (Hardware Security Module), which is used for random generating and storing the keys, as well as the operation of digital signing and encrypting the data with different cryptographic systems and algorithms.

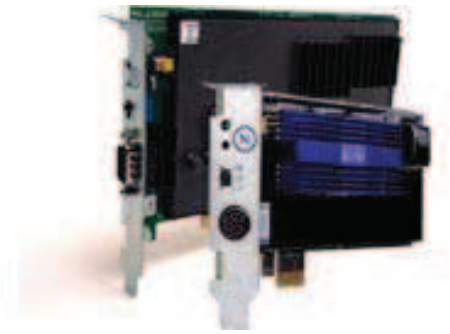

Figure 1: Embedded hardware security module

The HSM must be validated for FIPS-140-2 Level 3 or Common Criteria EAL4+. It also must support common Public key algorithms, as well as common symmetric algorithms. Our system connects to the HSM module through the PKCS#11.

II. MANDATORY CRYPTOGRAPHIC SYSTEMS AND ALGORITHMS

[4] Describes about mandatory common security mechanisms used in Digital Tachograph System.

A. Cryptographic Systems in MKD-CA

Vehicle units and tachograph cards use a classical RSA public-key cryptographic system to provide the following security mechanisms:

- Authentication between vehicle units and tachograph cards;
- transport of Triple-DES session keys between vehicle units and tachograph cards;
- digital signature of data downloaded from vehicle units or tachograph cards to external media.

Vehicle units and tachograph cards use a Triple DES symmetric cryptographic system to provide a mechanism for data integrity during user data exchange between vehicle units and tachograph cards, and to provide, where applicable, confidentiality of data exchange between vehicle units and tachograph cards.

B. Cryptographic Algorithms

RSA Algorithm used in this system is fully defined in [5]. Public exponent, e, for RSA calculations will be different from 2 in all generated RSA keys. The digital signature mechanisms use the SHA-1 hash algorithm as defined in [6]. TDES based algorithms is used in Cipher Block Chaining mode of operation described in [7].

C. Keys

RSA Keys are generated through three functional hierarchical levels:

- European level (ERCA Root)
- Member State level (MKD-CA Root)
- Equipment level (Card)

Member State root keys are certified by the European Certification Authority and Equipment public keys are certified by a Member State certification authority.
K_mWC TDES key is generated by ERCA, stored in MKD-CA and should be inserted in all workshop cards.
RSA Keys have the following length: modulus *n* 1024 bits, public exponent *e* 64 bits maximum, private exponent *d* 1024 bits. Triple DES keys are independent 64 bits long keys without setting error detecting bits.

D. Certificates

RSA Public key certificates are non self-descriptive Card Verifiable certificates [9]. The certificate content is shown on

Fig. 2. Certificate uniqueness in the MKD-CA domain is achieved with the CHR field of the certificates.
The certificate issued is a digital signature with partial recovery of the certificate content in accordance with [8], with the Certification Authority Reference appended (Fig. 4), and certificate content shown on Fig 3.

Field	Format	Bytes	Description
CPI	INTEGER	1	Certificate profile identifier ('01' for this version)
CAR	OCTET STRING	8	Certification authority reference
CHA	OCTET STRING	7	Certificate holder authorisation
EOV	TimeReal	4	Certificate end of validity. Optional, 'FF' padded if not used
CHR	OCTET STRING	8	Certificate holder reference
n	OCTET STRING	128	Public key (modulus)
e	OCTET STRING	8	Public key (public exponent)
		164	**Total bytes**

Figure 2: Certificate Content

$$Cc = \underset{106\ \text{Bytes}}{C_r} \;||\; \underset{58\ \text{Bytes}}{C_n}$$

Figure 3: Certificate Content for issuing the certificate

$$X.C = X.CA.SK['6A' \;||\; C_r \;||\; Hash(Cc) \;||\; 'BC'] \;||\; C_n \;||\; X.CAR$$

Figure 4: Certificate Issued

This certificate is 194 bytes long. CAR, being hidden by the signature, is also appended to the signature, such that the public key of the certification authority may be selected for the verification of the certificate. The certificate verifier shall implicitly know the algorithm used by the certification authority to sign the certificate.

E. Certificate Verification and Unwrapping

Certificate verification and unwrapping consists in verifying the signature in accordance with [8], retrieving the certificate content and the public key and verifying the validity of the certificate. If validity of the certificate passes, then the system checks the certificate End of validity date.

III. Securing the Interfaces

In [1] are shown MKD-CA Interfaces. Because of data sensitivity, we create several secured procedures to ensure data integrity and confidentiality. Interfaces from ERCA to MKD-CA and opposite, are strictly defined by ERCA in [3] and they are produced exactly they are defined, which is confirmed by [10] and [11] - signing session from ERCA to MKD-CA root certificate, as well as processing the KmWC request.

The main newly developed interface is the one that connects MKD-CA and MKD-CP, especially the part MKD-DPS from MKD-CP, which receives the highly sensitive data from MKD-CA (Private keys and PIN for workshop cards) and MKD-CIA, and prepares the data to be personalized on the tachograph card.

A. MKD-CA to MKD-CP Interface

We designed this interface to export the unexported data from the MKD-CA database into one file, such as each record in the file is the necessary data to be personalized into one digital tachograph cards. We prepare the data as TLV data, which are Tag / Length / Value.
We use here the encryption for assure the data integrity and confidentiality.

1) Data Integrity

Before the TLV data, we put information of the total length of the data, as well as KEK index, and after the TLV data we add MAC Key encrypted under KEK and calculated MAC over all data. The last one is unencrypted and is 4 Bytes long. MAC Key encrypted is 8 Bytes long. Here, KEK (Key Encryption Key) is defined with KEK index, one of several previously exchanged TDES keys.

2) Data Confidentiality

The data that should be personalized on every digital tachograph card consist some highly sensitive parts, such as certificate holder private key and PIN for workshop cards. According to [4] and Chinese Remainder Theorem, the system creates Prime number q, Prime number p, q_{Inv}, Exponent d_q, Exponent d_p and Public exponent e. The last is public, and all other private keys components are highly confidential. MKD-CA (HSM Module) shares the TDES keys with MKD-CP with common security shares keys, and encrypts these private key components with the shared TDES keys. HSM guarantee that TDES keys cannot be exported from the HSM. The system generates random 6 bytes character string PIN consisted only from digits, only for workshop digital tachograph card, which is also encrypted with the same TDES key.

IV. Conclusion

The designed digital tachograph system, especially MKD-CA, offers high level of security, as required in [3] and [4]. MKD-CA interfaces are designed to be reliable, available and secured to increase the security of the Digital Tachograph System as a whole.

The system offers high level of reliability and confidentiality, which is proved with the passed certification of the MKD-CA root certificate 27/11/2010 [11], as well as the passed interoperability tests [12] which made the system fully appropriate as the core CA system for Digital Tachograph System, not only in Macedonia, but in all other Memeber State Authority across Europe.

REFERENCES

[1] P. Ribarski, S. Ristov "Architectural and Design Overview of Digital Tachographs in Macedonia" *The 8th International Conference for Informatics and Information Technology (CIIT 2011)*, February, 2011.

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

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

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

[5] RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 2.0. October 1998.

[6] National Institute of Standards and Technology (NIST). SHA-1: FIPS Publication 180-1: Secure Hash Standard. April 1995.

[7] National Institute of Standards and Technology (NIST). TDES: FIPS Publication 46-3: Data Encryption Standard. Draft 1999.

[8] ISO/IEC 9796-2: Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997.

[9] ISO/IEC 7816-6: Information Technology — Identification cards — Integrated circuit(s) cards with contacts— Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.

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

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

[12] http://dtc.jrc.it/tachograph_cards_status.html