BASIC INFORMATION ABOUT SECURITY

Table of contents

1. DOCUMENT REVISION HISTORY

Rev: 01 Date of issue: 2017-09-20 Issued by: Arne Lohage

First issue.

Rev: 02 Date of issue: 2017-09-27 Issued by: Arne Lohage, Jan Eriksson

Second issue.

Rev: 03 Date of issue: 2017-10-06 Issued by: Arne Lohage, Leopold Schwinger

Added picture of Digital Tachograph Certificates, made and permitted by Leopold Schwinger (Intellic).

2. INTRODUCTION

For the Digital tachograph, the security requirements are the basic foundation for design, implementation and production. People who are experts in the field of security have no problem to argue for or against a specific solution. The challenge within those discussions could be that only a few persons really understand the topic.

This document is an attempt to explain the very basic parts of security that is related to the Digital tachograph.

3. RELEVANT DOCUMENTS

The appendices and documents listed below are of essential value for the understanding of this document.

Appendices

No.	Document no.	Title
/1/		
/2/		

Document

Ref.	Document no.	Title
[1]		Commission Regulation (EC) 1360/2002 of 13 June 2002 (Annex 1b)
[2]		

4. GLOSSARY

CIA triad	The CIA triad is the heart of information security. CIA is abbreviation for Confidentiality, Integrity and Availability.
Confidentiality	When talking about Confidentiality, one is talking about that the information shall only be accessible for authorized parties. When information is transferred from A to B, there is a risk that someone else than B can read the data; that threatens the confidence of the data. In order to enhance the confidence of the data, **encryption** is used.
Integrity	Integrity of information means to protect the information from being modified by unauthorized parties. The actual information is only valuable if it is correct. In order to enhance the integrity of the data, **signing** is used.
Availability	Availability of information is about ensuring that authorized parties get access to the information when needed. The information is valuable only if the right parties get it at the right time.
Authenticity	A component can prove its identity. **Signing** provides authenticity.
Non-repudiation	Non-repudiation means to ensure that a sender of a message has sent the message and the receiver of the message has received the message. Neither of the parties can later deny sending/receiving the message. Example: when A has sent a message and **signed** it, it is impossible later for A to deny he/she has sent it.
Certificates	Certificates are used to ensure correctness and trust in cryptographic keys. Certificates are used to establish the trust that can be put on Confidentiality, Integrity and Availability. Cryptographic keys and algorithms are used to enforce Confidentiality, Integrity and Availability. Regarding the Tachograph; the VU holds a root certificate. If we can use that root certificate to verify the certificate of a Tachograph Card, we can be pretty sure that it is a valid Tachograph Card.

5. BACKGROUND

5.1. History

In order to trust written information, a signature has been technically possible and used already since the time of Romans. Those signatures were used to certify the authenticity of the information so one can trust that the information is correct.

If you want only a certain group of people to be able to understand some information, you can use methods in order to restructure the text. Julius Caesar used an encryption algorithm “Caesar cipher” by exchanging each letter to the letter three steps ahead in the alphabet. It was enough to hold the information within a closed circle of people, thus creating confidentiality of the information.

Maria Stuart who was prisoned in UK during 16th century used special signs instead of letters. The secret police of that time could decrypt the messages after a careful analysis of how often a special sign appeared (frequency analysis). Some letters are more common than others and then it could be easily solved.

5.2. Modern time

The purposes with signatures and encryption is the same today as it was long ago; to be able to evaluate if the information is correct and to limit the access. Today more modern and advanced cryptology methods are used.

European Union decided 1999 that electronic signatures shall have the same legal status as a hand written one.

6. PUBLIC KEY INFRASTRUCTURE (PKI)

PKI is a collective name where advanced security techniques and juridical rules enable electronic signatures. PKI is based on asymmetric algorithms.

The technical ground pillars of a PKI infrastructure are digital signing, encryption and authentication which jointly together create a very strong protection of data information.

The foundation of a PKI infrastructure consists of a CA (Certificate Authority) which tasks are to issue and revoke certificates. A certificate is a list of unique attributes connected to a user. Through these unique attributes, the user can claim its identity.

6.1. Signing

An electronic signature is the solution to protect the integrity of the data; it shows a connection between the information and the sender.

Signing provides authenticity; it serves to ensure that B can trust that A is the sender and also for non-repudiation, i.e. A cannot deny that he/she is the sender.

A hash-algorithm is used to calculate an index value (hash value) based on the actual data. This hash value is encrypted and sent together with the data in clear text to the receiver. The receiver then

1) decrypts the index value and
2) also perform the hash-calculation on the open sent data.

Then the two hash values are compared (the own calculated and the decrypted from the sender). If they conform, everything is fine and the data is correct; otherwise the data has been modified, in worst case manipulated.

6.2. Encryption

Encryption is used to enhance the confidentiality of the data and limit the access for non-authorised people. The readable or understandable information becomes unreadable and the information must be decrypted in order to be understood.

Two types of encryption exist; symmetric encryption and asymmetric encryption.

6.2.1. Symmetric encryption

Only one private key is used, both by the sender and the receiver. The advantage is that it is fast and simple, but there is a challenge; how shall both users get access to the key in a secure way? It is vulnerable.

6.2.2. Asymmetric encryption

Asymmetric encryption uses two keys; one open **public key** and one closed **private key**. The public key is used by the sender to encrypt the data, and the receiver uses the private key to decrypt it. Only by using the private key one can decrypt the data, there is no other way.

The private key is secret (therefore private key is sometimes called secret key) and will never be shown. The public key and private key are mathematically related and it takes long time to find the private key based on the public key. With an adequate size of the key, it takes several hundred years to break the key even with today's computer capacity.

One advantage with asymmetric encryption is that fewer keys are needed and it is very useful when lots of keys need to be distributed (i.e. well suited for the Digital Tachograph system).

Example
Let us define:

- *m* – is a plain text that contains, for example, a hash digest or a message authentication code that can be calculated from the contents of m, or some other message received together with *m*.
- *s* – is the signature of *m*
- *c* – is the cipher text of *m*
- *X.PK* – is the public key of X
- *X.SK* is the private key of X

X uses the private key to **sign** a message *m* by computing:

$$s = X.SK[m]$$

Anyone in possess of the public key *X.PK* can verify that s was signed by X by computing $m = X.PK[s]$, because the private key is only known by X.

Anyone in possess of the public key *X.PK* can **encrypt** a message *m* by computing:

$$c = X.PK[m]$$

As X is the only party having access to the private key *X.SK*, only X is able to compute the plain text message *m*, by computing $m = X.SK[c]$.

6.3. Certificates

In real life, identification documents such as driving licence or passport are used to reduce frauds. In the digital world, similar controls of users and systems are used to validate the identity of receiver and sender of data.

A certificate is a digital list containing attributes that are used to authenticate and evaluate a user. The keys used when encrypting and decrypting are connected to the correct user by means of certificates.

Certificate Authority (CA) is a server that plays a huge role within PKI. Its main tasks are to issue and revoke certificates containing public keys. In order for the CA to issue a certificate, an authentication process between user and CA must be successfully done first.

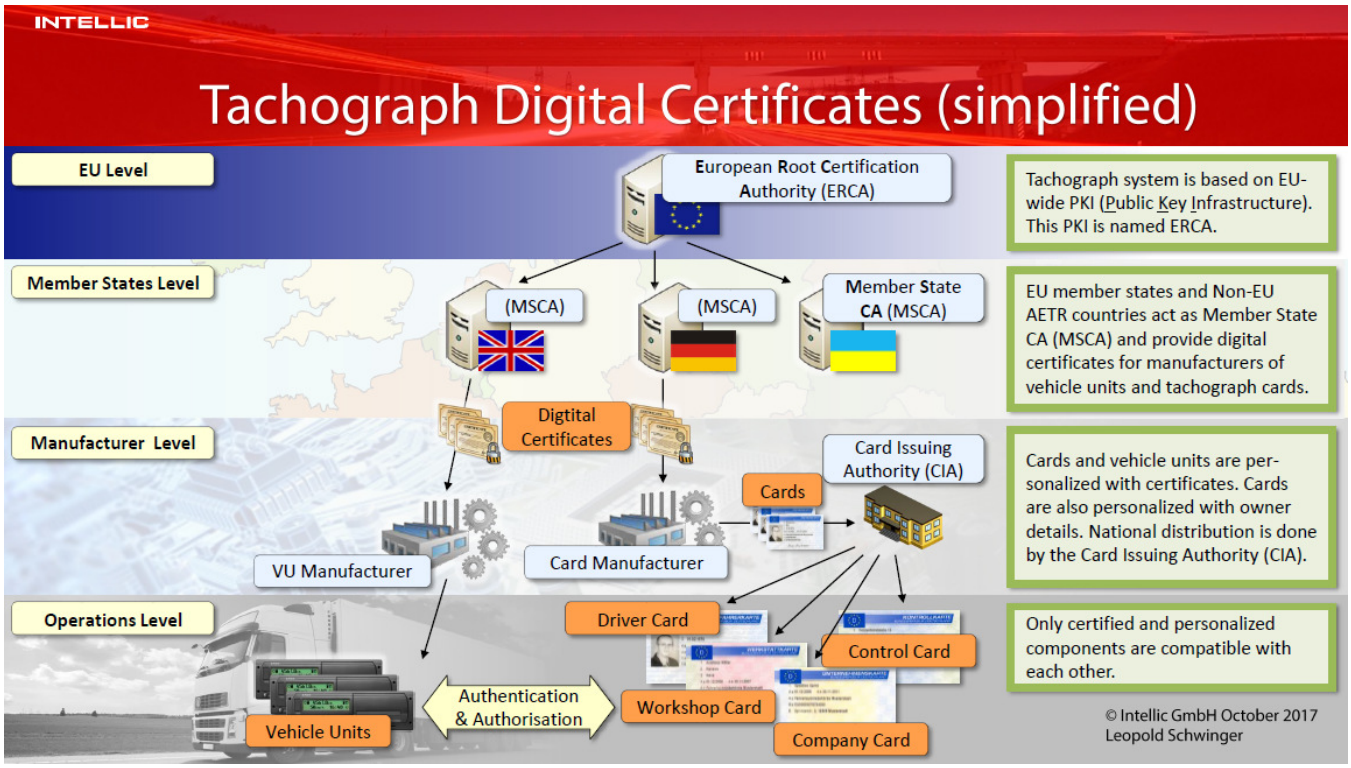
A CA is a trusted third party. All users trust that CA issues valid certificates.

Tachograph perspective
The certificates are used to trace public keys and signing authorities back to a common signing authority. If a certificate, i.e. the public key contained in the certificate, can be traced back to a common root certificate, then the public key in the equipment can be trusted.

A certificate is signed by the Certificate Authority's private key. The certificate contains identifiers that identify the public key contained in the certificate (e.g. Member State Public key), as well as the key that can be used to verify the certificate (e.g. European Public key). Thus, a certificate chain can be established.

Example in "real life"
Swedish authority applies for certificate from JRC by sending them the Member State public key and Member State identification. The response from European level (JRC) is then the Certificate of Member State (including Member State public key and certified by European private key) and the European public key. The European public key is then used to verify the Member State certificate.

This is why the root public key (ERCA in the case of the smart tachograph system) is installed in all entities that need to be trusted (VU, Tacograph Card, External GNSS).



7. IMPLEMENTING SECURITY IN TACHOGRAPHS

7.1. Overview

In order for enforcers and other users of tachographs to be able to trust the data, there are security requirements on the tachograph system. Basically, nothing is 100% secure for ever. What is common approach is to define what to protect (i.e. Target of Evaluation) and how much it should be protected (EAL = Evaluation Assurance Level). When this is defined for a system, for example the tachograph system, what is implemented and how it is implemented must be certified by an independent evaluator.

As an example, it is written in the Protection Profile document for the tachograph following:

> *Assurance level: EAL4 augmented with ATE_DPT.2 and AVA_VAN.5*

Protection Profile documents states *WHAT* to secure, the security documents describe *HOW*.

7.2. Security mechanisms for tachographs

For current existing Digital Tachographs, the security requirements are stated in Appendix 11 COMMON SECURITY MECHANISMS of ref [1].

Within this chapter of ref [1], the generalities are specified in chapter 1 as following (copied):

> *1. GENERALITIES*
> *This appendix specifies the security mechanisms ensuring:*
> *. the mutual authentication between VUs and tachograph cards, including session key agreement,*
> *. the confidentiality, integrity and authentication of data transferred between VUs and tachograph cards,*
> *. the integrity and authentication of data downloaded from VUs to external storage media,*
> *. the integrity and authentication of data downloaded from tachograph cards to external storage media.*

As seen from the text, it is assumed that the reader has a basic knowledge about the security vocabulary.

What is of interest to notify is that data exchanged between VU and card is encrypted (ensuring confidentiality) while the data is sent in clear text from both VU and card when downloaded to external storage media (only integrity and authentication are ensured).

7.3. Handling of keys

Implementing a PKI (Public Key Infrastructure) as described in this document above is in fact specified in ref [1] for the digital tachograph. In order to provide each component of the tachograph system with both a public and private key, there is a clear hierarchy defined. Starting from European level, it goes down to Member state level and further into equipment level.

Following text is copied from Appendix 11 of ref [1]:

> *CSM_006*
> *RSA keys shall be generated through three functional hierarchical levels:*
> *. European level,*
> *. Member State level,*
> *. Equipment level.*
>
> *CSM_007*

At European level, a single European key pair (EUR.SK and EUR.PK) shall be generated. The European private key shall be used to certify the Member States public keys. Records of all certified keys shall be kept. These tasks shall be handled by a European certification authority, under the authority and responsibility of the European Commission.

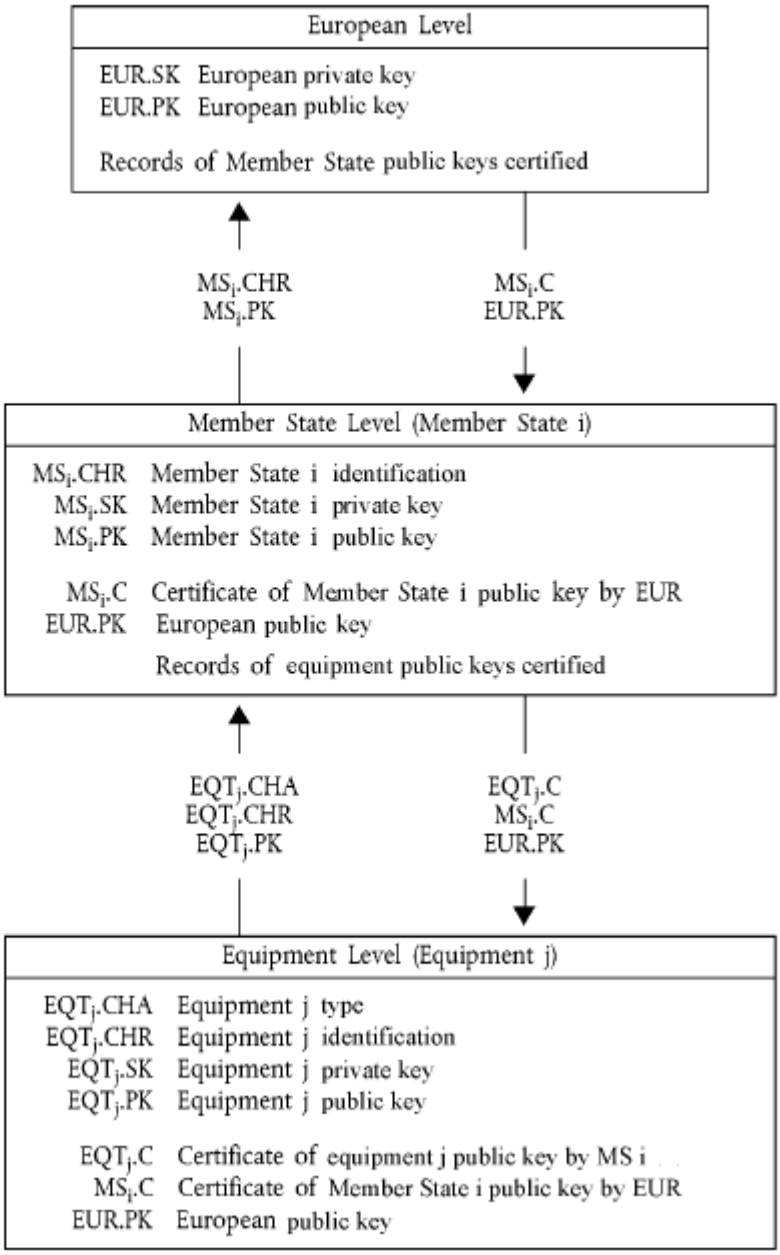
CSM_008
At Member State level, a Member State key pair (MS.SK and MS.PK) shall be generated. Member States public keys shall be certified by the European Certification Authority. The Member State private key shall be used to certify public keys to be inserted in equipment (vehicle unit or tachograph card). Records of all certified public keys shall be kept with the identification of the equipment to which it is intended. These tasks shall be handled by a Member State certification authority. A Member State may regularly change its key pair.

CSM_009
At equipment level, one single key pair (EQT.SK and EQT.PK) shall be generated and inserted in each equipment. Equipment public keys shall be certified by a Member State certification authority. These tasks may be handled by equipment manufacturers, equipment personalisers or Member State authorities. This key pair is used for authentication, digital signature and encipherement services

CSM_010
Private keys confidentiality shall be maintained during generation, transport (if any) and storage.

Following picture is copied from Appendix 11 of ref [1]:

The following picture summarises the data flow of this process:



7.4. ERCA and MSCA

At European level, JRC is responsible for the essential service European Root Certification Authority (ERCA) which oversees the digital security of the tachographs and generates the electronic certificates.

At Member state level and for Sweden, Transportstyrelsen is responsible for the service Member State Certification Authority (MSCA). Stoneridge as a tachograph manufacturer receives keys from Transportstyrelsen in a secure way and the keys are downloaded into each and every tachograph that is produced.

The rules about handling certificates and keys are defined in what is called *ERCA policy*.