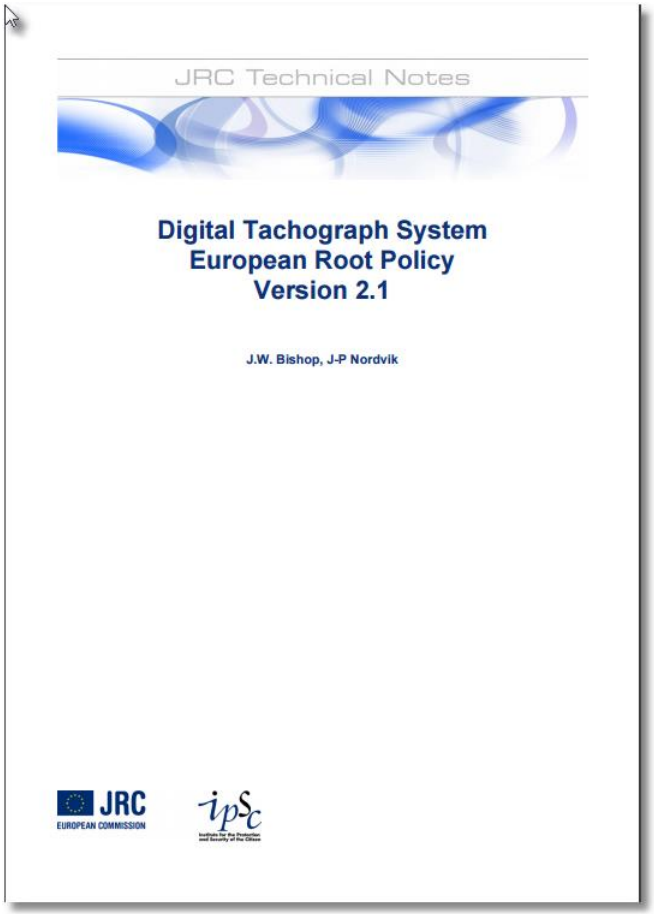
Legal status of “Digital Tachograph System, European Root Policy, Version 2.1”

ERCA POLICY



DG JRC manages, on behave of DG MOVE two major services:

- the European Root Certification Authority (ERCA) and
- the Laboratory for Interoperability Certification

These services have been set up and are currently operated by JRC/IPSC in fulfillment of the duties assumed by the European Commission with **Council Regulation 2135/98**, Annex I(B); Appendix 11 requirement 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**."

ERCA POLICY

European Commission

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

DIRECTORATE E - Inland Transport
The Director

Brussels, 23 SEP. 2004
TREN E4/HH/LH/ik (D) 17052

NOTE FOR THE ATTENTION OF MR. CADIOU,
DIRECTOR OF THE INSTITUTE FOR THE PROTECTION AND SECURITY OF THE CITIZEN,
JOINT RESEARCH CENTRE, ISPRA

Subject: Statement of compliance concerning the ERCA system

With regard to the organisation and execution of the ERCA key ceremony, please find enclosed the requested statement of compliance concerning the ERCA system, issued by the European Authority.

I would like to take this opportunity to thank you again for your commitment and cooperation in this important file.

Heinz Hilbrecht

Copy MM. Hutchins (ADMIN), Lamoureux, Ristori, Mayet (TREN)

Enclosure: Statement of compliance concerning the ERCA system

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11
Office: DM28 1/75. Telephone: direct line (32-2) 296.84.56. Fax (32-2)296.53.72
Internet: http://europa.eu.int/comm/dgs/energy_transport/index_en.html

Statement of compliance concerning the ERCA system

Having regard to

- Requirements CSM_007 and CSM_008 of Annex 1B[1] to Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport, as last amended by Council Regulation (EC) No 2135/98;

Digital Tachograph System - European Root Policy version 1.0, issued by the Joint Research Centre and accepted by the Director General for Energy and Transport on 12 December 2003 (ref. TREN/E1/LH/03-460), as last amended by version 2.0;

Digital Tachograph System - Certification Practices Statement version 0.7, issued by the Joint Research Centre on 21 September 2004;

- Report on the Functional Testing of the ERCA Signing System, issued by the Joint Research Centre on 22 September 2004,

ERCA System Inspection Report No 1, version 1.0, issued by ADMIN/DS/4 on 17 August 2004 as a result of the first security review of the ERCA system;

ERCA System Inspection Report No 2, version 1.0, issued by ADMIN/DS/4 on 21 September 2004 as a result of the second security inspection of the ERCA system;

the undersigned hereby confirms that the Joint Research Centre can proceed with the organisation and execution of the key ceremony, on 24 September 2004 at the JRC premises in Ispra.

The key ceremony will indicate that the procedures are implemented according to their description.

On execution of the key ceremony, the ERCA system can go into operation. If for any reason, there is a failure in any of the procedures involved at the key ceremony, the process of generation of keys will be suspended. As a consequence, the operational phase will also be postponed.

Heinz Hilbrecht
Director Inland Transport

[1] Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, OJ L207 of 5.8.2002.

ERCA POLICY

European Commission

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

DIRECTORATE E - Inland Transport
The Director

Brussels, 12 DEC. 2003
TREN/E1/LH/03-460
D(2003) 22073

NOTE TO THE ATTENTION OF MR LAMOUREUX,
DIRECTOR-GENERAL

Subject: your agreement to send the final version of the European Root Certification Authority (ERCA) policy document to the EU Member States and to the Joint Research Centre.

Please find enclosed to this note the European Root Certification Authority (ERCA) policy document.

The main objective of the ERCA policy document is to describe the obligations of the European and national authorities, which are responsible for the management (generation, approval and certification) of the European and national security keys for the digital tachograph and the smart cards. It will thus establish the basis for the future activities of the certification authorities, both on European and national level. In this respect we also envisage a new Administrative Arrangement with the JRC on the deployment of the ERCA policy.

The ERCA policy document has been prepared at our request by the Joint Research Centre in Ispra. The JRC prepared this document in cooperation with representatives of the Member States, the national security experts of the so-called Card Issuing Working Group.. Attached to this note is a letter of the chairman of this Task Force, Mr. Janin of the French Ministry of Transport, in which it is confirmed that the ERCA policy document ensures the security needs of the digital tachograph project.

The ERCA policy is in line with the technical requirements laid down in Annex 1B (Commission Regulation (EC) No 1360/2002[1]). Appendix 11 of the Annex 1B is dedicated to the common security mechanisms, which include the security key management of the digital tachograph system. According to these requirements the key management consists of the generation of a single European security key pair and the use of a European private key to certify Member States public keys. These tasks shall be

[1] Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, OJ L 207 of 5.8.2002

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Office: DM26 - 04/50 . Telephone: direct line (32-2) 2958174. Fax: (32-2) 2995887.
Internet: http://europa.eu.int/comm/dgs/energy_transport/index_en.html

handled by a European root certification authority, under the authority and responsibility of the European Commission.

We ask your agreement to send the ERCA policy as the final version to the Member States, so that it can be used for the implementation of the European and national security certification policies, and to the JRC, to be published as a final version on the their public website.

Heinz Hilbrecht

Approval Director-General 12 XII

Annex: - Digital Tachograph System – European Root Policy version 0.9

- Letter from Mr. Janin, chairman of Task Force 3 (security issues) of the Card Issuing Working Group

C.C.: Messrs. Van Vreckem, Onestini, Poucet, Bishop

Joint Research Centre

ERCA POLICY
CHANGE PROCEDURE

European Commission

8 ERCA POLICY CHANGE PROCEDURES

8.1. The only changes that may be made to this policy without notification are editorial or typographical corrections.

8.2. Changes which the ERCA may make to this policy with notification to the MSAs but without comments from the MSAs are changes to the contact details.

8.3. All other changes to the ERCA policy shall be made only after notification to, and the receipt of comments from, the ERCA and the MSAs, according to the following procedure:

a) The MSAs or the ERCA shall submit proposals for change to the ERCA policy to the European Authority.

b) The European Authority shall distribute proposals to change the ERCA policy to the MSAs and to the ERCA.

c) The European Authority shall set an appropriate period for comments.

d) The MSAs and the ERCA may comment on the proposed changes within the defined period for comments.

e) The European Authority shall consider the comments and shall decide which, if any, of the notified changes to implement.

f) The European Authority shall notify the MSAs and the ERCA about its decision, and shall set an appropriate period for the changes to be implemented.

ERCA POLICY CHANGE EXAMPLE

European Commission

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for the Protection and Security of the Citizen
Non-proliferation and Nuclear Safeguards Unit
T.E.M.P.E.S.T Laboratory
TP 361
I-21020 Ispra (Va)

TEMPEST Laboratory

ERCA Policy Change Proposal 5

Date of Issue: **26th April 2004**

Description

CP#5 replaces CP#1 in the light of comments received by the ERCA from Member State authorities.

This CP concerns the definition of specific security measures for the digital tachograph root key management processes, and the removal of references to the formal security classification scheme defined in the *Commission Provisions on Security* (Commission Decision No.2001/844/EC, ECSC, Euratom of 29th Nov. 2001; Official Journal of the European Communities L 317 of 03.12.2001).

Rationale

Reference to EU security classifications requires formal accreditation of IT systems handling classified information by the Commission security accreditation authority (DG-ADMIN / DS4).

An estimate of the minimum time required to complete the accreditation process provided by DG-ADMIN / DS4 during November 2003 was 24 months. This delay is clearly beyond the current implementation deadlines.

Removal of explicit references to the Commission provisions on security from the ERCA policy also facilitates transfer of the ERCA service to an organisation outside the Commission.

List of Changes

1. Section 4.1.1: replace existing text:

   The operational procedures of the ERCA conform to the *Commission Provisions on Security* [8] (see also Section 4.4 ERCA Asset Classification below).

with the following text:

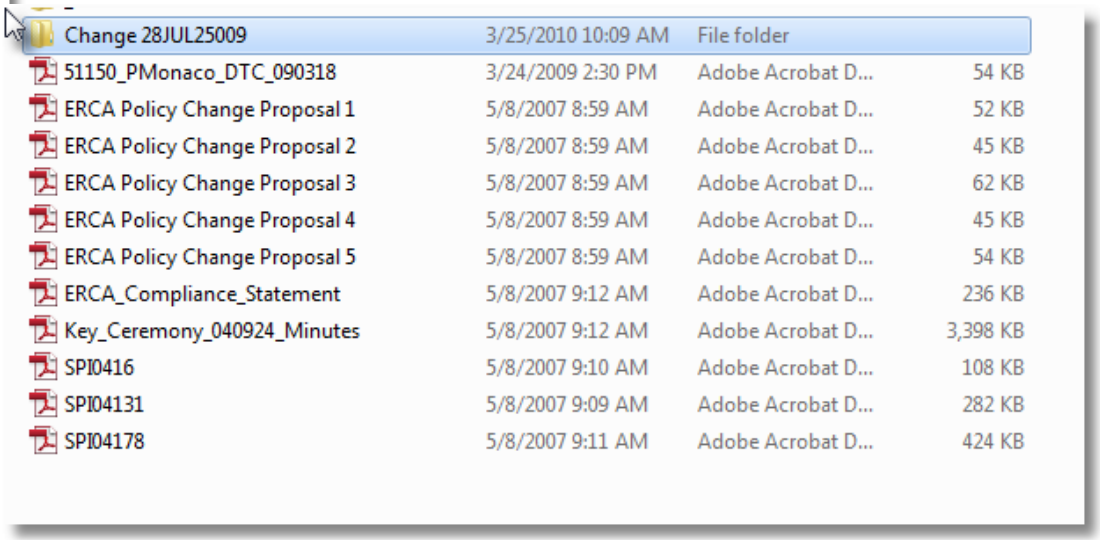
   The ERCA implementation shall conform with the best practices described in ISO 17799 – *Information technology – Code of practice for information security management* [8].

2. Section 4.4: replace the existing text:

   The column Security Classification contains the EU security classification described in the *Commission Provisions on Security* [8]. Four levels of security classification are defined:

   EU Top Secret: This classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of its Member States.

   EU Secret:This classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States.



Change 28JUL25009	3/25/2010 10:09 AM	File folder	
51150_PMonaco_DTC_090318	3/24/2009 2:30 PM	Adobe Acrobat D...	54 KB
ERCA Policy Change Proposal 1	5/8/2007 8:59 AM	Adobe Acrobat D...	52 KB
ERCA Policy Change Proposal 2	5/8/2007 8:59 AM	Adobe Acrobat D...	45 KB
ERCA Policy Change Proposal 3	5/8/2007 8:59 AM	Adobe Acrobat D...	62 KB
ERCA Policy Change Proposal 4	5/8/2007 8:59 AM	Adobe Acrobat D...	45 KB
ERCA Policy Change Proposal 5	5/8/2007 8:59 AM	Adobe Acrobat D...	54 KB
ERCA_Compliance_Statement	5/8/2007 9:12 AM	Adobe Acrobat D...	236 KB
Key_Ceremony_040924_Minutes	5/8/2007 9:12 AM	Adobe Acrobat D...	3,398 KB
SPI0416	5/8/2007 9:10 AM	Adobe Acrobat D...	108 KB
SPI04131	5/8/2007 9:09 AM	Adobe Acrobat D...	282 KB
SPI04178	5/8/2007 9:11 AM	Adobe Acrobat D...	424 KB

ERCA POLICY LAST UPDATE V 2.0 –> V 2.1

European Commission

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

DIRECTORATE E - Inland Transport
Land transport policy

28 JUIL. 2009

Brussels,
TREN-E1/AK/nl D(2009) 40140

NOTE TO THE ERCA MEMBER STATE AUTHORITIES

Subject: **ERCA Policy for the Digital Tachograph: Change in Audit Procedure**

Dear Sir/Madam,

In my letter of 18th September 2008, Member State Authorities and the Joint Research Centre were invited to comment on proposals made by the Netherlands to change the frequency of audits as set out in the European Root Key Certification Authority (ERCA) Policy Document (version 2.0).

The proposed changes would require that paragraph 5.3.44 of the ERCA policy is amended so that the first audit carried out by Member State authorities would take place 12 months after the implementation, and that, thereafter (assuming that the first had been successful), Member State authorities would carry out further audit operations at intervals of not more than 36 months. In case of a fundamental change of a part of the operations covered by the approval policy, the Member State Authority would audit that part within 12 months after implementation.

The outcome was that a total of eight Member States responded. Seven replied positively to the changes proposed by the Netherlands, and that such a modification would not jeopardise security, whilst the eighth rejected the proposal because they believed that the security of the system would be in danger of being compromised, since the long gap between audits would mean that problems may not be detected at an appropriate time.

The Joint Research Centre (JRC), acting as the European Root Certification Authority have also noted some concerns with the proposal made by the Netherlands. Since ERCA is driven mainly by a need to retain a high level of security, JRC have considered that a reduction in the frequency of audit reports to every 36 months will not maintain the appropriate level of security. JRC also note that a number of Member States continue to fail to provide any audit reports, which is also a threat to the overall security.

Commission européenne, B-1049 Bruxelles - Belgique. Téléphone: (32-2) 299 11 11.
Bureau: DM24 02/46. Téléphone: ligne directe (32-2) 2981913. Télécopieur: (32-2) 29552165.
E-mail: philippe.chantraine@ec.europa.eu

Joint Research Centre

However, JRC have considered that it would be acceptable to increase the interval between audits, after a successful audit, from 12 to 24 months, in order to make more national resources available for other security-related tasks, such as, for instance, roadside checks, workshop inspections and the exchange of best practice, as have recently been developed through the Commission Regulation, Directive and Recommendation related to detection and prevention of frauds, and which were adopted on 23rd January 2009.

Given the introduction of these initiatives to help Member States, DGTREN, acting as the European Authority, supports the recommendation and notes that the provisions in the ERCA policy document do not preclude Member States carrying out audits at a greater frequency if they wish to do so.

Therefore, the Commission has amended the ERCA Policy Document so as to allow audits to be carried out at 24 month intervals, after the first successful audit. Furthermore, in the event of non-conformities being detected, the frequency of an audit will revert back to every 12 months. The new version of the ERCA Policy Document is attached and will become effective from the date of this letter.

A. MAYET

Szabolcs Schmidt
Head of Unit

Encl.: 1

c.c: Jean-Pierre Nordvik (JRC)
James Bishop (JRC)
Dominique Landat (JRC)
Philippe Chantraine (TREN)

ERCA POLICY LEGAL BASIS CONCLUSIONS

- The ERCA POLICY V 1.0 has been written in cooperation with Member States representatives, and by a group of MS security experts, a task force so-called Card Issuing Working Group, and formally endorsed/adopted by DG MOVE (ex TREN) in 2003. It entered into force in 2004.

- The ERCA policy evolves according precise change rules, starting from:

  1. Mandate to the Commission in the regulation
  2. Approval and adoption of the V1.0 as Reg. implementing document
  3. V1.0 in chapter 8 lists the Change Procedure rules
  4. All the rules have been respected until the last up-date leading to the V2.1

* *
*

Thank you for your attention.

Joint Research Centre (JRC)
Web: www.jrc.ec.europa.eu