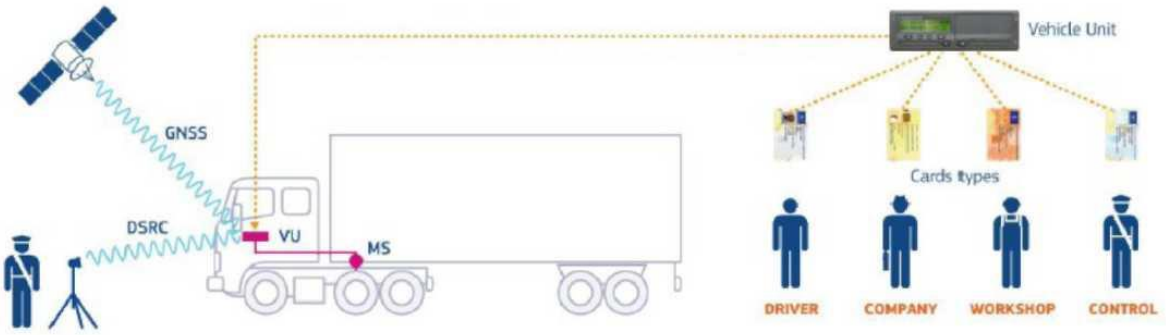
Republic of Serbia

Ministry of Construction, Transport and Infrastructure

Smart Tachograph NA Policy of the Republic of Serbia (ST-SRB-NA Policy V 1.1)



Amendment History

Version Control	Issue Date	Status
Version 1.0	May 2021	Initial version for release to ERCA
Version 1.1	October 2021	Corrections, inclusion of remarks from JRC and inclusion appointed SRB-CP and SRB-CA

Contents

1 Introduction

1.1 Overview

The second-generation Digital Tachograph system, called Smart Tachograph, has been introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council.

Annex IC of Commission Implementing Regulation (EU) 2016/799 lays down the technical requirements for the construction, testing, installation, operation and repair of Smart Tachographs and their components. Appendix 11 (Common Security Mechanisms) of Annex IC specifies the security mechanisms ensuring:

- Mutual authentication between different components of the tachograph system.
- Confidentiality, integrity, authenticity and/or non-repudiation of data transferred between different components of the tachograph system or downloaded to external storage media.

Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realize this for the second-generation tachograph system.

A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic system relies on master keys that must be delivered to the relevant actors. An infrastructure consisting of three layers has been set up. At the European level, the European Root Certification Authority (ERCA) is responsible for the generation and management of root public-private key pairs, with the respective certificates, and symmetric master keys. The ERCA issues certificates to National Certification Authorities (SRB-CA) and distributes symmetric master keys to the MSCAs. The MSCA is responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment.

This document forms the Certificate Policy (CP) for the PKI of the Serbian Certification Authority (SRB-CA). It lays down the policy at NA level for key generation, key management and certificate signing for the Smart Tachograph system, based on the ERCA Certificate Policy. For the SRB-CA to issue certificates and/or symmetric keys to component personalizers SRB-CP, they shall comply with requirements also laid down in this document.

This document follows the framework for CPs described in RFC 3647.

How the SRB-CA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the SRB-CA Certification Practice Statement (CPS) for the Smart Tachograph system. Digital Tachograph (first generation system) and Smart Tachograph (second generation system) are two different systems that must be run in parallel and independently. For this reason, separate NA policies have to be maintained to avoid problems when in the future the time comes to discontinue the Digital Tachograph and its corresponding ERCA (Gen 1). For this reason, the "Serbian policy for the Digital Tachograph System" will stay in place in addition to this SRB-NA Policy.

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119.

1.2 Responsible organisations

The authority responsible for implementation of the SRB-NA policy, referred to as SRB-NA (Serbian National Authority), is

Ministry of Construction, Transport and Infrastructure
Department for Road Transport, Roads and Road Safety
Nemanjina 22-26 str.
11000 Belgrade
Republic of Serbia

The appointed SRB-CIA is:

Road Safety Traffic Agency (RTSA)
Mihaila Pupina 2 av.
11000 Belgrade
Republic of Serbia

The appointed SRB-CA is:

National Bank of Serbia
The Institute for Manufacturing Bank Notes and Coins – Topčider
Pionirska street 2
11000 Belgrade
Republic of Serbia

The appointed SRB-CP is:

National Bank of Serbia
The Institute for Manufacturing Bank Notes and Coins – Topčider
Pionirska street 2
11000 Belgrade
Republic of Serbia

The SRB-CA or SRB-CP may subcontract parts of its processes to subcontractors, Service Agencies. The use of Service Agencies in no way diminishes the SRB-CA's or SRB-CP's overall responsibilities.

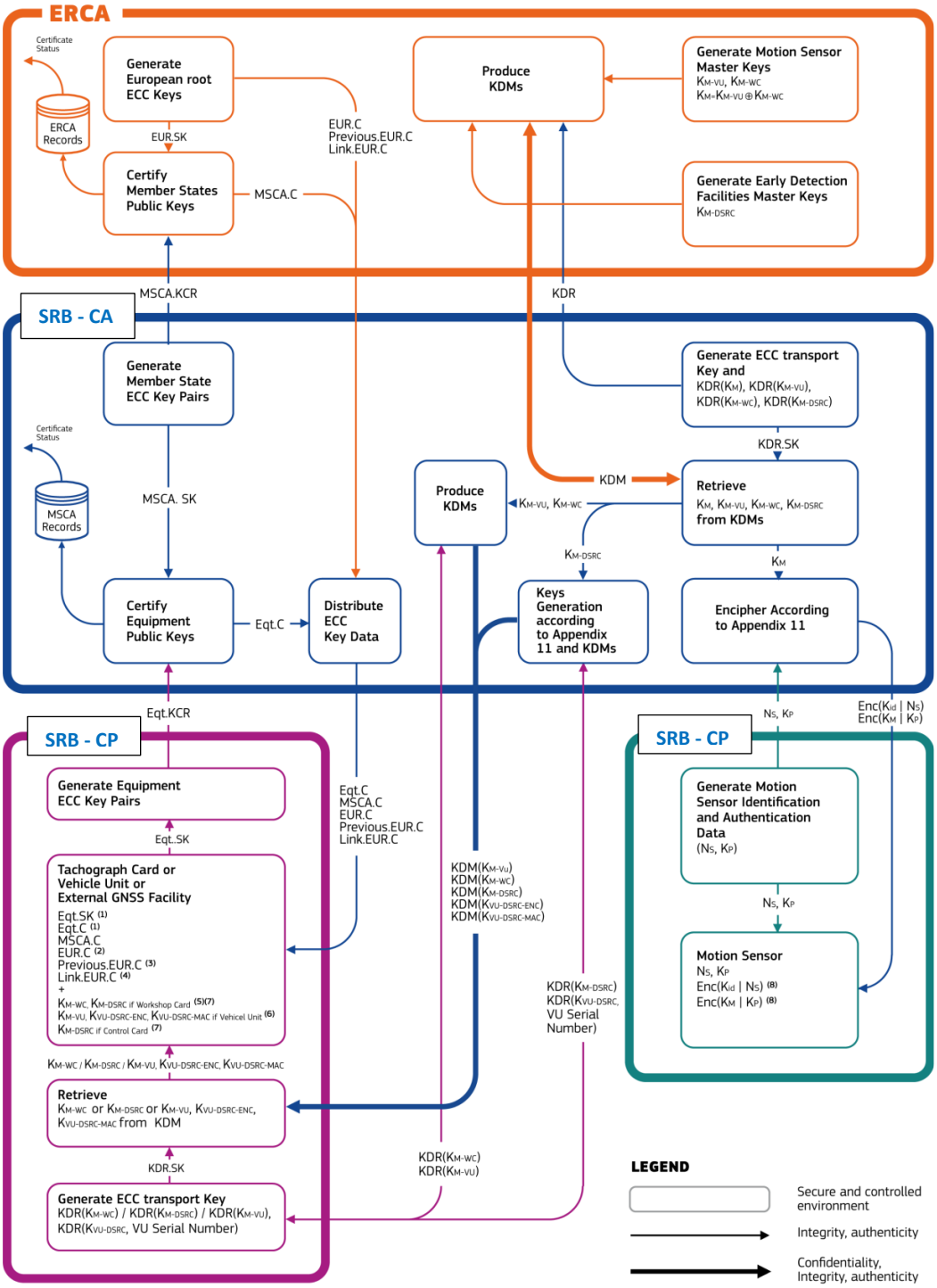
1.3 Document Name and Identification

This document is named " Smart Tachograph NA Policy of the Republic of Serbia". This Certificate Policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the certificates used in the Smart Tachograph system do not contain a reference to this policy. The current version can be found at the beginning of this document. **Version 1.1.** of this policy was endorsed by the ERCA (see section 1.5.1) on **25th of November 2021. Ref. Ares(2021)7275663 – 25/11/2021.**

1.4 PKI Participants

The participants in the Smart Tachograph PKI and in the Symmetric Key Infrastructure are described here and represented in Figure 1. Figure 1 also represents the exchanges between the participants, namely ERCA, MSCAs and component personalizers SRB-CP.

For more information on the symmetric and asymmetric keys mentioned in this section, refer to Appendix 11 Part B.



NOTES

1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Figure 1 Smart Tachograph PKI and Symmetric Key Infrastructure

1.4.1 Certification Authorities

1.4.1.1 European Root Certification Authority (ERCA)

The ERCA is the root Certification Authority (CA) that creates and assigns public key certificates in the PKI. It operates the following component services:

Registration service, certificate generation service, dissemination service.

The ERCA generates PKI root key pairs and respective certificates, along with link certificates to create a chain of trust between different root certificates.

The ERCA is also the entity generating, managing and distributing on request the symmetric master keys, i.e. the Motion Sensor Master Key-VU part ($K_{M\text{-}VU}$), the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC}$) and the DSRC Master Key ($K_{M\text{-}DSRC}$).

1.4.1.2 Certification Authority of the Republic of Serbia (SRB-CA)

The SRB-CA operates as sub-CA under the ERCA. It creates and assigns public key certificates for equipment. For this, it operates a registration service, certificate generation service and dissemination service. The SRB-CA receives the certificate requests from component personalizers SRB-CP and disseminates the certificates to these parties for the issuance of Card certificates, called MSCA Card key pair. The SRB-CA requests MSCA certificates from the ERCA, because of its responsibility regarding the issuance of Card certificates. The SRB-CA also requests symmetric master keys from the ERCA and $K_{M\text{-}WC}$ and $K_{M\text{-}DSRC}$ to card personalizers.

1.4.2 Registration Authorities

1.4.2.1 Card Issuing Authority of the Republic of Serbia (SRB-CIA)

SRB-CIA is determined by the SRB-NA.

SRB-CIA responsible for:

- appoints a SRB-CA and SRB-CP;
- verifying whether all required documents were produced;
- verifying whether all prerequisites for the issuing of a tachograph card subject to the Regulation (EU) No 165/2014 of the European Parliament and of the Council, Annex IC of the Commission Implementing Regulation (EU) 2016/799, all other relevant legal provisions, the ERCA Policy and this SRB-NA-Policy are fulfilled;
- verifying whether a tachograph card was already issued to the applicant in another EU-member state;
- verifying that the user of each tachograph card is identified at some stage of the card issuing process;
- ensuring that the applications data is transmitted to the SRB-CP properly according to the produced documents and to the requirements of this policy;
- informing all users about the requirements of this policy in an appropriate manner;

- ensuring that the PIN of the workshop card is handed over only to the intended bearer of the workshop card by using separate recipients for workshop card (workshop) and PIN (named technician);
- immediately informing the SRB-NA and the SRB-CA or one of its authorized agencies about all security-relevant incidents.

1.4.2.2 SRB-CA Registration Authority

The SRB-CA ensures within its authority, that a proper registration of component manufacturers and card personalizers SRB-CP takes place before issuing of a certificate, distribution of symmetric keys or encrypting device data. The registration process is detailed in the CPS.

1.4.3 Subscribers

The only subscribers to the SRB-CA public key certification service are the component personalizers SRB-CP. Component personalizers SRB–CP are responsible for the personalization of:

- Tachograph Cards: four different types of tachograph cards exist: driver cards, company cards, workshop cards and control cards.

- The driver cards and workshop cards have two key pairs and corresponding certificates issued by an MSCA_Card, namely
    - a key pair and certificate for mutual authentication, called Card_MA;
    - a key pair and certificate for signing, called Card_Sign.

The workshop cards also contain $K_{M\text{-}WC}$ and $K_{M.DSRC}$ with key length of all possible VUs - with regard to the used cipher suites.

- The company and control cards have a key pair and corresponding certificate issued by an MSCA_Card for mutual authentication.

The control cards also contain $K_{M\text{-}DSRC}$ with key length of all possible VUs - with regard to the used cipher suites.

Component personalizers SRB-CP are responsible for ensuring the equipment is provided with the appropriate keys and certificates.

1.4.3.1 Personalizer of Serbian Tachograph Cards (SRB-CP)

- Requirements regarding vehicle unit and motion sensor manufacturers are currently not covered by this policy. This policy must be adapted if the need arises.
- ensures generation of the two card key pairs, for mutual authentication and signing, for driver and workshop cards;
- performs the certificate application process with the SRB-CA_Card for driver and workshop cards;
- performs the application for $K_{M\text{-}WC}$ and $K_{M\text{-}DSRC}$ (workshop cards only);

- ensures availability of keys and certificates in the card for mutual authentication and signing, MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only);
- ensures generation of the card key pairs for mutual authentication for company and control cards;
- performs the certificate application process with the SRB-CA_Card for company and control cards;
- performs the application of $K_{M\text{-}DSRC}$ (control cards only);
- ensures availability of keys and certificates in the card for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only).

1.4.4 Relying Parties

Parties relying on the SRB-CA certification services are primarily the Serbian authorities tasked with enforcing the rules and regulations regarding driving times and rest periods, especially the Serbian police.

The SRB-CA certifications are used within the system to validate the authenticity of equipment certificates, which in turn are used to validate the authenticity of data downloaded from Vehicle Units and driver cards. Other directly relying parties are component manufacturers- and personalizers, CIA's, drivers, companies and workshops.

1.5 Key and Certificate Usage

The SRB-CA shall use its SRB-CA private keys only for:

- Signing of certificate signing requests (see section 4.1.1)
- Issuing Certificate Revocation Lists, if such a method is used for providing certificate status information.

The SRB-CA shall use the symmetric master keys solely to derive VU-specific keys and encrypt motionsensor related data as specified in Annex IC Appendix 11.

The SRB-CA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to component personalizers SRB-CP by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11.

The SRB-CA_Card certificates shall be used to verify card certificates issued by the SRB-CA_Card.

The Card_MA certificates shall be used for mutual authentication and session key agreement between Card and VU.

The Card Sign certificates shall be used to verify the authenticity and integrity of data downloaded from the card. The Card_Sign private key may only be used to sign data downloaded from the card. All valid versions of K_M shall be used by the SRB-CA to encrypt MoS pairing keys K_P, and to derive all valid versions of the MoS identification key K_{ID}. All valid versions of K_{ID} shall be used by the SRB-CA to encrypt MoS serial numbers. $K_{M\text{-}VU}$ and $K_{M\text{-}WC}$ shall be provided to component personalizers SRB-CP for their installation respectively in VUs and Workshop Cards. KM-VU shall be used by the VU together with the corresponding KM-WC to generate the right KM during VU-MoS pairing.

$K_{M\text{-}DSRC}$ shall be used by the SRB-CA to derive VU specific keys to secure the DSRC communication. $K_{M\text{-}DSRC}$ shall be used by control and workshop cards to derive the VU specific DSRC keys required to decipher and verify the authenticity and integrity of the VU's DSRC communication.

1.6 Policy Administration

1.6.1 ERCA

The European Commission service responsible for implementation of the certification policy at the European level and for the provision of key certification and key distribution services to the Member States is referred to as the European Root Certification Authority (ERCA).

The contact address of the ERCA is:

Head of the Cyber and Digital Citizens' Security Unit E3

Directorate E - Space, Security and Migration

Joint Research Centre (TP 580)

European Commission

Via Enrico Fermi, 2749

I-21027 Ispra (VA)

The ERCA reviews the MSA certificate policies, including this SRB-NA certificate policy, for conformity with the requirements defined in the ERCA certificate policy. The objective of the review process is to assure comparable levels of security in each Member State. The ERCA archives the policy review reports and the NA certificate policies for reference purposes.

The ERCA provides key certification services to the MSCAs affiliated to an MSA only if the outcome of the MSA certificate policy review provides sufficient grounds to judge that the requirements in the ERCA certificate policy will be met. Continuation of key certification service from the ERCA to an MSCA depends on timely receipt of the MSA audit reports (see section 8.1) demonstrating that the MSCA is continuing to fulfil its obligations as laid down in the approved MSA certificate policy.

1.6.2 SRB-NA

Republic of Serbia appointed Ministry of Construction, Transport and Infrastructure (Law on working hours of crews of vehicles engaged in road transport and tachographs, Official Gazette of RS, no. 96/15 and 95/18) as Member state authority SRB-NA.

The SRB-NAs responsibilities are:

- Laying down and documenting an NA certificate policy in conformance with all applicable requirements in the ERCA certificate policy and taking care of its approval by the ERCA. The SRB-NA makes an English version of the SRB-NA certificate policy available to the ERCA and takes care for a Serbian version.
- Approving the CPS of the SRB-CA and stating its compliance with this Policy. This can be accomplished in conjunction with the compliance audits of the SRB-CA (see chapter 8).

- Ensuring or arranging that the SRB-NA-Policy is made available to all authorities involved.
- Ensuring that the SRB-CA has the resources required to operate in conformity with this certificate policy.
- Approval of SRB-CA, SRB-CP, SRB-CIA security policies.
- Requre that any relevant prescription mandated by the Common Criteria security certification of the equipment is met during the complete life cycle of the equipment.

1.6.3 SRB-CA

The SRB-CIA appoints SRB-CA, which implements the Serbian certification policy and provides key certification and key distribution services to the component personalizers SRB-CP in Serbia.

The SRB-CA documents its implementation of the SRB-NA certificate policy in a Certification Practice Statement (SRB-CA CPS). The SRB-CA CPS is the SRB-CAs procedural document, which details how the SRB-NA certificate policy is enforced in day-to-day management. The document is developed and owned by the SRB-CA. It shall be treated as restricted information. The SRB-CA shall make the contents of its CPS available on a need-to-know basis only. The SRB-CA CPS shall be managed, reviewed, and modified following document control procedures.

SRB-NA certificate policy require that the issuance process of tachograph cards ensures that the effective date of the card's certificate(s) is equal to the begin of the validity of the tachograph card itself, as encoded in EF Identification.

SRB-NA certificate policy require that the ERCA is notified without delay of loss, theft, or potential compromise of any SRB-CA private key or symmetric master key and indicate any follow-up investigation and potential action by the NA.

The SRB-CA makes its CPS available to the SRB-NA. The SRB-NA is responsible to determine whether the SRB-CA CPS complies with the SRB-NA certificate policy. Upon request, the SRB-CA also makes a version of its CPS available to the ERCA.

The SRB-CA maintains records of its operations as appropriate to demonstrate conformity with the SRB-NA certificate policy and shall make these records available to the SRB-NA and/or the ERCA on demand. Complaints from component personalizers SRB-CP about the services provided by the SRB-CA shall be addressed to the SRB-NA (contact address see 1.5.2).

1.7 Definitions and Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CP	Certificate Policy
CPS	Certification Practice Statement
SRB-CA	Certification Authority of the Republic of Serbia
SRB-CIA	Card Issuing Authority of the Republic of Serbia
SRB-CP	Personalizer of Serbian Tachograph Cards
SRB-NA	Serbian National Authority
SRB-NA-CP	Serbian National Authority Certificate Policy
DSRC	Dedicated Short Range Communications
CSR	Certificate Signing Request
EC	European Commission
ECC	Elliptic Curve Cryptography
EGF	External GNSS Facility
EA	European Authority
ERCA	European Root Certification Authority
ERCA - CP	European Root Certificate Policy and Symmetric Key Infrastructure Policy
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISMS	Information Security Management System
ISSO	Information System Security Officer
JRC	Joint Research Centre
KDR	Key Distribution Request
K_M	Motion Sensor Master Key
$K_{M\text{-}VU}$	VU part of K_M
$K_{M\text{-}WC}$	WC part of K_M

Acronym	Definition
K_{ID}	Motion Sensor Identification Key
K_P	Motion Sensor Pairing Key
$K_{M\text{-}DSRC}$	DSRC Master Key
LKM	Labeled Key Message
MA	Mutual Authentication
MoS	Motion Sensor
NA	National Authority
NCP	Normalized Certificate Policy
PKI	Public Key Infrastructure
RFC	Request for Comment
RSA	Rivest, Shamir und Adleman
TC	Tachograph Card
VU	Vehicle Unit
WC	Workshop Card

Further definitions may be found in the documents referenced by this SRB-CA certificate policy; see the section References towards the end of this document.

2 Publication and Repository Responsibilities

2.1 Repositories

- All equipment certificates issued by the SRB-CA shall be maintained in the SRB-CA database.

2.2 Publication of Certification Information

- The SRB-NA shall publish this Certification Policy on the his website
- The SRB-CA Certification Practice Statement shall not be public but shall be communicated on request to the relevant parties.

2.3 Time or Frequency of Publication

- Information relating to changes in this policy shall be published according to the schedule defined by the change (amendment) procedures laid down in section 9.12 of this document.

2.4 Access Controls on Repositories

- All information available via the website shall have read-only access. The SRB-CA shall designate staff having write or modify access to the information in the SRB-CA CPS.
- All information published on the website shall be available via a secure Internet connection.

3 Identification and Authentication

This chapter describes how identification and authentication (I&A) shall take place for initial and re-key certificate requests and for symmetric key distribution requests between the SRB-CA and the ERCA. I&A between the SRB-CA and equipment manufacturers or card personalizers is detailed in the SRB-CA CPS.

3.1 Naming

3.1.1 Types of Names

3.1.1.1 Certificate Subject and Issuer

The Certification Authority Reference and Certificate Holder Reference identify the issuer and subject of a certificate. They shall be formed in the following way as described in Annex IC, Appendix 11, CSM_136/CSM_141 and Appendix 1:

Entity:

- SRB-CA

Identifier:

- Certification Authority Key Identifier (KID)

Construction:

- Nation numeric
- Nation alpha
- Key serial number
- Additional info
- CA identifier

Test key certificates, test certificate requests, test key distribution requests and test key distribution messages for the purpose of Interoperability Tests, shall contain the values '54 4B' ("TK") in the *additionalInfo* field.

3.1.1.2 Key Distribution Requests and Key Distribution Messages

Key Distribution Requests and Key Distribution Messages are identified by the key identifier of the ephemeral public key generated by each MSCA, see section 4.2.1. The key identifier value is determined according to section 3.1.1.1 with the following modifications:

- keySerialNumber: unique for each requesting entity
- additionalInfo: '4B 52' ("KR", for Key Request), unless it concerns a test KDR. In that case, '54 4B' ("TK", for Test Key) shall be used.

3.2 Initial Identity Validation

3.2.1 Method to prove Possession of Private Key

When submitting certificate signing requests (CSRs) to the ERCA, proof of possession of the corresponding private key via an internal signature, as specified

in section 4.1.1, is necessary. The CSRs may also have an outer signature proving the authenticity of the message. The outer signature shall be produced by an already certified private key referenced in the CSR.

By verification (done manually together with the MSA/MSCA), if a hash calculated over the received CSR matches the hash over the CSR sent by the MSCA (as described in the ERCA CPS), additional prove of integrity, authenticity and initial trust is established.

3.2.2 Authentication of Organization Identity

The SRB-CA defines a procedure for the authentication of organization identities (e.g. equipment manufacturers) in its CPS.

3.2.3 Authentication of Individual Identity

The SRB-CA defines a procedure for the authentication of individual identities. The procedure is documented in the SRB-CA's CPS.

3.2.4 Validation of Authority

The SRB-CA shall define a procedure for the validation of authority in its Certification Practice Statement.

3.2.5 Criteria for Interoperation

The SRB-CA shall not rely on any external certificate authority except the ERCA for the certificate signing and key distribution services it provides to the smart tachograph system.

If the SRB-CA must rely on an external PKI for any other service or function, review and approval of the CP and/or CPS of the external certification service provider by the SRB-NA prior to applying for certification services, is required.

3.3 I&A for Re-Key Requests

The Identification and Authentication procedures for re-key requests (see sections 4.1.8 and 4.2.9) shall be the same as those described in section 3.2.

3.4 I&A for Revocation Request

Certificate revocation requests received by the ERCA from any source (see section 4.1.10) shall be validated by direct communication with the MSA responsible for the certificate-holding MSCA, through the contact point.

The SRB-CA describes in its CPS how it will validate certification revocation requests for equipment certificates, if certificate revocation procedures are available.

4 Life-Cycle Operational Requirements for Certificates, symmetric Keys and Encryption Services

This chapter describes the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates, symmetric keys for cards and VUs and equipment data encryption services between the SRB-CA and its component personalizers SRB-CP as well as for the application and distribution of MSCA certificates and symmetric master keys between the ERCA and the SRB-CA.

4.1 SRB-CA Public Key Certificate Application and Issuance

4.1.1 Certificate Signing Requests

Certificate signing requests can only be submitted by MSCAs recognized by their MSA via a compliance statement (see 1.5.2).

A CSR shall be in TLV-format. Table 1 shows the CSR encoding, including all tags. For the lengths, the DER encoding rules specified in ISO/IEC 19790 shall be used. The values are specified in the remainder of this section.

Data Object	Req	Tag
Authentication	c '67'	
ECC (CV) Certificate	m	'7F 21'
Certificate Body	m	'7F 4E'
Certificate Profile Identifier	m	'5F 29'
Certification Authority Reference	m	'42'
Certificate Holder Authorisation	m	'5F 4C'
Public Key	m	'7F 49'
Standardized Domain Parameters OID	m	'06'
Public Point	m	'86'
Certificate Holder Reference	m	'5F 20'
Certificate Effective Date	m	'5F 25'
Certificate Expiry Date	m	'5F 24'
Inner Signature	m	'5F 37'
Certification Authority Reference of Outer Signature Signatory	c	'42'
Outer Signature	c	'5F 37'

Table 1 Certificate signing request format

m: required
c: conditional

The **Authentication** data object shall only be present in case the Outer Signature data object is present.

The version of the profile is identified by the **Certificate Profile Identifier.** Version 1, specified in section 7.1, shall be identified by a value of '00'.

The **Certification Authority Reference** shall be used to inform the ERCA about the ERCA private key that the SRB-CA expects to be used for signing the certificate. For Certification Authority Reference values see section 3.1_. At any given time, the key identifier of the ERCA root key available for signing will be indicated on the ERCA website.

The **Certificate Holder Authorisation** shall be used to identify the type of certificate. It consists of the six most significant bytes of the Tachograph Application ID ('FF 53 4D 52 44 54'), concatenated with the type of equipment for which the certificate is intended (Annex IC, Appendix 11, CSM141). For MSCA certificates, the equipment type shall be set to '0E' (14 decimal).

The **Public Key** nests two data objects:

- The **Domain Parameters** data object shall reference the standardized domain parameters to be used with the public key in the certificate. It shall contain one of the object identifiers specified in table 1 of Appendix 11, Annex IC.
- The **Public Point** data object shall contain the public point. Elliptic curve public points shall be converted to octet strings as specified in ISO/IEC 18033-2. The uncompressed encoding format shall be used (Annex IC, Appendix 11, CSM_143).

The **Certificate Holder Reference** is used to identify the public key contained in the request and in the resulting certificate. The Certificate Holder Reference shall be unique. It can be used to reference this public key in equipment-level certificates (Annex IC, Appendix 11, CSM_144). For Certificate Holder Reference values see section 3.1.

The **Certificate Effective Date** shall indicate the starting date and time of the validity period of the certificate. The **Certificate Expiration Date** shall indicate the end date and time of the validity period. Both data elements shall be of data type TimeReal, specified in Annex IC, Appendix 1. Note that the validity period defined by these two data elements shall be either 17 years and 3 months (for MSCAVU-EGF certificates) or 7 years and 1 month (for MSCACard certificates).

The certificate body shall be self-signed via an **Inner Signature** that shall be verifiable with the public key contained in the certificate request. The signature shall be created over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116, using the hashing algorithm linked to the size of the public key in the CSR as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

The **Certification Authority Reference of Outer Signature Signatory** shall indicate the MSCA and the respective key that placed the outer signature. It shall only be present in case an outer signature is present. For possible values, see section 3J_.

The **Outer Signature** shall be absent if the SRB-CA applies for its initial certificate. The outer signature shall be required if the SRB-CA applies for a successive certificate. In this case, the Certificate Signing Request shall be additionally signed via an outer signature by the SRB-CA, using one of its current valid SRB-CA private keys. The outer signature authenticates the request. Because the SRB-CA is subscribed to receive both MSCA_Card and MSCA_VU-EGF certificates, the outer signature shall be placed using a private key linked to a certificate of the same type.

The Outer Signature shall be created over the encoded ECC (CV) Certificate (including the certificate's tag '7F 21' and its length) and the Certification Authority Reference of Outer Signature Signatory field (including the certificate's tag '42' and its length). The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116 using the hashing algorithm linked to the size of the SRB-CA key used for signing, as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

The SRB-CA shall calculate and store a hash over the complete CSR, using the hashing algorithm linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50. This hash will be used by the ERCA together with the MSA/MSCA to manually verify the authenticity of the CSR, see section 4.1.2.1.

4.1.2 Certificate Application Processing

4.1.2.1 Verification of CSR contents

The ERCA ensures that a CSR originating from any MSCA is complete, accurate, and duly authorized. The ERCA only signs an MSCA certificate if this is the case.

Checks for correctness, completeness and authorization are performed manually by the ERCA officers and/or in an automated way by the ERCA registration service. If the request is correct and complete, the ERCA officers authorize the signing of an MSCA certificate.

For each CSR it receives, the ERCA verifies that

- the transport media is readable; i.e. not damaged or corrupted;
- the CSR format complies with Table 2;
- the request is duly authorized. If an outer signature is in place, the ERCA verifies the correctness of this signature. In any case, the ERCA contacts the MSCA as described in the ERCA CPS and verifies that a hash calculated over the received CSR matches the hash over the CSR sent by the MSCA;
- the MSCA is entitled to receive the requested type of certificate;
- the Certification Authority Reference contained in the request indicates the ERCA root private key currently valid for signing MSCA certificates;
- the Certificate Holder Reference is unique. For MSCAs the Certificate Holder Reference is a Certification Authority Key Identifier (KID). The Key Serial Number in this KID shall differ between keys of the same MSCA, making the KID unique;
- the domain parameters specified in the request are listed in Table 1 of Annex IC, Appendix 11, and the strength of these parameters matches the strength of the ERCA root key indicated in the Certification Authority Reference;

- the public point in the request has not been certified by the ERCA previously and has not been used as an ephemeral key for symmetric key distribution previously (see section 4.2.3), even for interoperability test purposes;
- the public point in the request is on the curve indicated in the request;
- the inner signature can be verified using the public point and the domain parameters indicated in the request. This proves that the MSCA is in possession of the private key associated with the public key;
- the outer signature is present if the request is not for the initial MSCAVU-EGF or MSCACard certificate of the MSCA;
- If present, the outer signature can be verified using the public point and the domain parameters in the MSCA certificate referenced in the Certification Authority Reference of Outer Signature Signatory field. Moreover, the private key usage period of this key has not expired yet.

If any of these checks fails, the ERCA rejects the CSR. The ERCA communicates the rationale for any request rejection to the MSCA and the responsible MSA.

4.1.2.2 Certificate generation, distribution and administration

If all checks succeed, the ERCA proceeds to sign the certificate as described in section 4.1.3.

The following information is recorded in the ERCA database for each certificate signing request received:

- the complete CSR originating from the MSCA;
- the complete resulting public key certificate, if any;
- the standardized domain parameters OID and the public point of the certified public key;
- the certificate effective data and certificate expiration date;
- the Certificate Holder Reference (for identification of the public key);
- the hash over the binary certificate data, if any. The hash length shall be linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50;
- the hash over the binary CSR data, see section 4.1.1;
- the certificate status "Valid" if the certificate is issued or "Rejected" in case the CSR is rejected;
- a timestamp.

The MSCA certificate(s) are written to transport media in accordance with the requirements in section 4.1.4, for return to the MSCA. Every certificate copy written on transport media is verified afterwards using the ERCA public key. The ERCA also writes a copy of the ERCA public key certificate that can be used to verify the MSCA certificate(s) to the transport media.

After successful distribution of a new MSCA certificate, the ERCA updates the certificate status information in the ERCA repository. No other notification action is performed. The ERCA retains the transport media with the CSR and archives it in

their controlled premises. The ERCA aims to complete public key certification operations within one working day. The time required for the ERCA to supply a MSCA public key certificate or distribute a symmetric key shall be determined solely by the time required for correct execution of the ERCA procedures. A turnaround time of one month is guaranteed. When requesting a certificate, MSCAs shall take into account this maximum turnaround time.

4.1.3 Certificates

The format of the MSCA public key certificates can be found in section 7_1.

The ERCA creates the signature over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116, using the hashing algorithm linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

4.1.4 Exchange of Requests and Responses

For transportation of certificate signing requests and certificates, CD-R media should be used:

- The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA accepts and dispatches CSRs and certificates as e-mail attachments.

The SRB-CA shall write three copies of each certificate signing request to the transport medium for transport to the ERCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

The ERCA writes three copies of each certificate to the transport medium for return to the SRB-CA. These copies are in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

Each certificate signing request and certificate shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS. Another paper copy of the data shall be held by the ERCA or the SRB-CA, respectively.

For both CSRs and certificates, the transport media and the printouts are handed over between an ERCA employee and the SRB-CAs courier in the ERCA controlled area.

4.1.5 Certificate Acceptance

The courier signs for receipt of the SRB-CA certificate at the ERCA premises.
Upon reception of the certificate at the SRB-CA premises, the SRB-CA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the certificate complies with Table 9 in section 7.1;
- all certificate field values match the values requested in the CSR;
- the certificate signature can be verified using the ERCA public root key indicated in the CAR field.

If any of these checks fail, the SRB-CA shall abort the process and contact the ERCA. Certificate rejection is managed according to the certificate revocation procedure (see section 4.1.10).

4.1.6 Key Pair and Certificate Usage

The SRB-CA shall use any key pair and the corresponding certificate in accordance to section 6.2.

4.1.7 Certificate Renewal

Certificate renewal, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.1.8 Certificate Re-key

Certificate re-key means the signing of a new SRB-CA certificate, in replacement of an existing certificate. Certificate re-key shall take place either:

- When the SRB-CA is nearing the end of the usage period of (one of) its private key(s). In this case, re-key shall be done in a timely manner to ensure that the SRB-CA can continue operations after the end of this period;
- Following certificate revocation.

Certificate application, processing, issuance, acceptance and publication are the same as for the initial key pair. The SRB-CA shall immediately distribute the necessary keys and certificates to the component personalizers SRB-CP as further described in the SRB-CA CPS.

The MSCA key pair(s) may be changed regularly. The ERCA shall not impose any limits on the number of MSCA certificates that it will sign. MSCAs shall be allowed to request multiple MSCA certificates of the same type, if justified for its activity, with overlapping validity periods.

4.1.9 Certificate Modification

Certificate modification is not allowed.

4.1.10 Certificate Revocation and Suspension

4.1.10.1 Circumstances for certificate revocation

SRB-CA certificates shall be revoked in the following circumstances:

- rejection on receipt of a newly issued certificate (see section 4.1.5);
- compromise or suspected compromise of a SRB-CA private key;
- loss of a SRB-CA private key;
- SRB-CA termination;
- SRB-NA or SRB-CA failure to meet obligations under the Regulation and the ERCA certificate policy.

4.1.10.2 Who can request revocation

The ERCA considers revocation requests originating from the following entities as authoritative:

- the European Authority;
- all NAs;
- all recognized MSCAs;

The European Authority is authorized to request revocation of any MSCA certificate. An MSA is authorized to request revocation for certificates issued to the MSCAs listed in its MSA certificate policy.

An MSCA is authorized to request revocation for certificates issued to itself. The ERCA shall reject revocation requests originating from any other entity.

4.1.10.3 Procedure for revocation request

The certificate revocation procedure is described in the SRB-CA CPS.

4.1.10.4 Revocation request grace period

The grace period for certificate revocation is five working days from the start of the circumstances for revocation, within which a subscriber shall make a revocation request.

4.1.10.5 Time within which ERCA shall process the revocation request

The ERCA processes correct, complete and authorized revocation requests within three working days of receipt.

4.1.10.6 Revocation checking requirements for relying parties

Relying parties shall be responsible for checking the certificate status information published in the ERCA repository.

4.1.10.7 Certificate status issuance frequency

The status of ERCA and MSCA public key certificates are retrievable online from https://dtc.irc.ec.europa.eu/. The ERCA maintains the integrity of the certificate revocation status information.

Certificate status information published in the ERCA repository shall be updated on the first working day of each week.

4.1.10.8 Maximum latency for CRLs

Not applicable.

4.1.10.9 On-line revocation / status checking availability

The revocation / status information published in the ERCA repository is only guaranteed to be available during normal working hours.

4.1.10.10 On-line revocation / status checking requirements

No stipulation.

4.1.10.11 Other forms of revocation advertisements available

None.

4.1.10.12 Special requirements concerning key compromise

Private key compromise is a security incident that shall be processed.

If one of the SRB-CA private keys is compromised or suspected to be compromised, the SRB-CA shall report the incident to the ERCA and to the SRB-NA without unnecessary delay and at least within 8 hours of detection. In their notification, the SRB-CA shall indicate the circumstances under which the compromise occurred.

The follow-up investigation and potential action by the SRB-NA and/or SRB-CA shall be taken to reduce the risk of misuse of a compromised key.

The outcome of the SRB-NA investigation shall be reported to the ERCA.

4.1.11 Certificate suspension

Certificate suspension is not allowed.

4.1.12 Certificate Status Service

The availability of the website mentioned in section 4.1.10.7 is guaranteed during normal working hours. A list of MSCA certificate status information is also downloadable from this website in a common file format (e.g. .csv, Excel).

4.1.13 End of Subscription

Subscription for the ERCA's certificate signing services ends when the SRB-NA decides for SRB-CA termination. Such a change is notified to the ERCA by the SRB-NA as a change to the SRB-NA certificate policy.

In the case of subscription ending, the decision to submit a certificate revocation request for any valid SRB-CA certificates, or to allow all SRB-CA certificates to expire, is in the responsibility of the SRB-NA.

4.1.14 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that SRB-CA root private keys will never be exported to or stored in any system apart from the SRB-CA production and fallback systems.

4.2 Symmetric Master Key Application and Distribution between the ERCA and the SRB-CA

The following requirements are closely based on the respective chapter of the ERCA Gen. 2 certificate policy.

4.2.1 Key Distribution Requests

Key distribution requests can only be submitted by MSCAs recognized by their MSA via a compliance statement (see 1.5.2).

A KDR shall be in TLV-format. Table 2 shows the KDR encoding, including all tags. For the length, the DER encoding rules specified in ISO/IEC 19790 shall be used. The values are specified in the remainder of this section.

Data Object	Req	Tag
Key Distribution Request	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorization	m	'83'
Key Identifier	m	'84'
Public Key (for ECDH key agreement)	m	'7F 49'
Standardized Domain Parameters OID	m	'06'
Public Point	m	'86'

Table 2 Key distribution request format

The version of the profile is identified by the **Request Profile Identifier.** Version 1, specified in Table 2, shall be identified by a value of '00'.

The **Message Recipient Authorization** shall be used to identify the symmetric key that is requested. It consists of the concatenation of

- the six most significant bytes of the Tachograph Application ID ('FF 53 4D 52 44 54'),
- the type of key that is requested (see below, 1 byte),
- the version number of the requested master key (1 byte).

The following values shall be used to indicate the type of key requested:

- '07': K_M, motion sensor master key
- '27': $K_{M\text{-}WC}$, motion sensor master key workshop part
- '67': $K_{M\text{-}VU}$, motion sensor master key VU part
- '09': $K_{M\text{-}DSRC}$, DSRC master key

The **Key Identifier** is a unique 8-byte octet string identifying the public key presented in the KDR for ECDH key exchange, see section 4.2.3. Its value is determined according to section 3.1.1.2. Since a MSCA shall use a different ephemeral key pair for every key distribution request, the SRB-CA may use the key identifier to keep track of the ephemeral private key to be used for the decryption of a particular key distribution message, once it arrives at the SRB-CA. For that reason, the ERCA copies the key identifier in the key distribution message, see Table 3

The **Public Key** nests two data elements:

- The data element Public Point shall contain the public point of the ephemeral SRB-CA key pair to be used for key agreement. The SRB-CA shall convert the public point to an octet string as specified in ISO/IEC 18033-2, using the uncompressed encoding format.
- The data element Domain Parameters shall contain the object identifier of the set of standardized domain parameters to be used in conjunction with the public point. For more information, see section 4.2.3.

The SRB-CA shall calculate and store a hash over the complete KDR, using the hashing algorithm linked to the key size of the requested master key, as specified in

Annex IC, Appendix 11, CSM_50. This hash will be used by the ERCA to verify the authenticity of the KDR, see section 4.2.2.1.

4.2.2 Master Key Application Processing

4.2.2.1 Verification of KDR contents

The ERCA ensures that a KDR originating from an SRB-CA is complete, accurate, and duly authorized. The ERCA only creates a key distribution messages if this is the case.

Checks for correctness, completeness and authorization are performed manually by the ERCA officers and/or in an automated way by the ERCA registration service. If the request is correct and complete the ERCA officers may authorize the generation of a key distribution message by the key distribution service. For each KDR it receives, the ERCA verifies that

- the transport media is readable; i.e. not damaged or corrupted;
- the KDR format complies with Table 2
- the request is duly authorized. The ERCA contacts the SRB-CA as described in the ERCA CPS and verifies that a hash calculated over the received KDR matches the hash over the KDR stored by the SRB-CA (see the end of section 4.2.1);
- the SRB-CA is entitled to receive the requested type of master keys:
    - o SRB-CAs responsible for issuing tachograph cards shall be entitled to receive all valid versions of $K_{M\text{-}WC}$ with regard to used cipher suite and the DSRC master key $K_{M\text{-}DSRC}$;

4.2.2.2 KDM generation, distribution and administration

If all checks succeed, the ERCA proceeds to prepare the key distribution message by determining the symmetric key requested by the SRB-CA and following the steps as described in section 4.2.3 (from step 2). The following information is recorded in the ERCA database for each key distribution request received:

- the complete KDR originating from the SRB-CA;
- the complete resulting key distribution message, if any;
- the standardized domain parameters OID, the ephemeral public point and the key identifier;
- the key type and version of the master key;
- the hash over the binary key distribution message data, if any. The hash length shall be linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50;
- the hash over the binary KDR data, see section 4.2.1;
- the status "Distributed" in case the key is distributed to the SRB-CA or "Rejected" in case the KDR is rejected;
- a timestamp.

The ERCA retains the transport media with the KDR and archives it in their controlled premises.

Once the key distribution message has been generated, the ERCA sends it to the MSCA as specified in section 4.2.5.

The ERCA aims to complete key distribution operations within one working day. Turnaround time of one month is guaranteed. When requesting distribution of a key, SRB-CAs shall take into account this maximum turnaround time.

4.2.3 Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys distributed by the ERCA to SRB-CAs is protected via an Elliptic Curve Integrated Encryption Scheme (ECIES). This scheme allows for agreement between the ERCA and SRB-CA on encryption keys and MAC keys to be used to protect the master symmetric keys during distribution. The ECIES has been standardized in ISO/IEC 18033-2. The ECIES variant to be used for ERCA symmetric key distributions uses the following cryptographic algorithms, in accordance with Appendix 11 of Annex IC:

- Key derivation function: KDF2, as specified in ISO/IEC 18033-2;
- Message authentication code algorithm: AES algorithm in CMAC mode, as specified in NIST, Special Publication 800-38B;
- Symmetric encryption algorithm: AES in the Cipher Block Chaining (CBC) mode of operation, as defined in ISO/IEC 10116.

On a high level, the ECIES consists of the following steps. More details are given for each step below:

1. The MSCA generates a unique ephemeral ECC key pair for Diffie-Hellman key agreement and sends the public key to the ERCA in the Key Distribution Request, see Table 2
2. The ERCA similarly generates a unique ephemeral ECDH key pair and uses the Diffie-Hellman key agreement algorithm together with its own private key and the MSCA's ephemeral public key to derive a shared secret.
3. Using the key derivation function, the shared secret and additional information detailed below, the ERCA derives an encryption key and a MAC key.
4. The ERCA uses the encryption key to encrypt the symmetric key to be distributed.
5. The ERCA uses the MAC key to calculate a MAC over the encrypted key.

Step 1

For the generation of its ephemeral public key used for Diffie-Hellman key agreement, the SRB-CA shall choose one of the standardized domain parameters from Table 1 of Annex IC, Appendix 11. The strength of the chosen set of domain parameters shall match the length of the requested symmetric key, according to CSM_50 in Appendix 11. Ephemeral key pair generation shall take place in an HSM complying with the requirements in section 6.2. The ephemeral private key shall never leave the HSM.

After generating the ephemeral key pair, the SRB-CA shall convert the public point to an octet string as specified in ISO/IEC 18033-2. The uncompressed encoding format shall be used. The SRB-CA shall include the OID of the chosen standardized domain parameters and the octet string representing the public point in the KDR, which is sent to the ERCA.

Step 2

The ERCA generates an ephemeral key pair, using the standardized domain parameters specified in the received KDR. The ERCA shall use the ECKA-DH algorithm as defined in ISO/IEC 18033-2 together with its own ephemeral private key and the SRB-CA's ephemeral public key to derive a shared point (K_x, K_y). The ERCA shall check that this point is not the infinity point. If it is, the ERCA shall generate a new ephemeral key pair and try again. Otherwise, the ERCA shall form the shared secret K by converting Kx to an octet string as specified in ISO/IEC 18033-2.

Ephemeral key pair generation shall take place in an HSM complying with the requirements in section 6.2. The ephemeral private key shall never leave the HSM.

Step 3

For deriving the encryption key K_{ENC} and the MAC-ing key K_{MAC}, the ERCA uses the key derivation function KDF2(x, l) defined in ISO/IEC 18033-2. The octet string x shall be equal to the shared secret K from the previous step. The hash function that is necessary to instantiate the KDF2 function shall be linked to the length of the symmetric key to be distributed, as described in Appendix 11 CSM_50.The output length l shall be equal to the output length of this hash function.

Given the output O of this key derivation function, the encryption and MAC-ing keys shall be formed as

- K_{ENC} = first L octets of O
- K_{MAC} = last L octets of O

where L is the required length of K_{ENC} and K_{MAC} in octets, in accordance to Appendix 11 CSM_50.

Step 4

If necessary (i.e. for a 192-bytes key), the ERCA pads the symmetric key to be distributed using padding method 2 defined in ISO/IEC 9797-1. Subsequently, the ERCA encrypts the padded key with AES in the Cipher Block Chaining (CBC) mode of operation, as defined in ISO/IEC 10116, using K_{ENC} with an interleave parameter m = 1 and an initialization vector SV consisting of binary zeros:

Encrypted symmetric key = AES-CBC(symmetric key + padding if necessary, K_{ENC})

Step 5

The ERCA concatenates the encrypted symmetric key with a string S, which is the concatenation of the values of the Message Recipient Authorization and the Key Identifier used in the key distribution message (see section 4.2.4)

S = Message Recipient Authorization || Key Identifier

Using K_{MAC}, the ERCA then computes a MAC over the concatenation of the Encrypted symmetric key and S, using the AES algorithm in CMAC mode, as specified in NIST Special Publication 800-38B. The length of the MAC shall be linked to the length of the AES session keys, as specified in Appendix 11 CSM_50.

MAC = AES-CMAC (Encrypted symmetric key || S, K_{MAC})

Any operations with the ephemeral private key, with the shared secret and with the derived keys K_{ENC} and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2.

The ERCA shall record the value of S and of the MAC. As described in section 4.2.6, the SRB-CAs will use these values to verify the authenticity of the key distribution message.

4.2.4 Key Distribution Messages

After performing the Master Key application processing (see section 4.2.2), the ERCA shall construct a key distribution message as shown in Table 3 For the lengths, the DER encoding rules specified in (ISO/IEC 8825-1 shall be used. The values are specified in the remainder of this section.

Data Object	Req	Tag
Key Distribution	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorization	m	'83'
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	m	'84'
Public Point of the ERCA for ECDH key agreement	m	'86'
Encrypted symmetric key	m	'87'
MAC	m	'88'

Table 3 Key distribution message format

The version of the profile is identified by the **Request Profile Identifier**. Version 1 specified in Table 3 shall be identified by a value of '00'.

The **Message Recipient Authorisation** shall be identical to the Message Recipient Authorisation data element in the KDR from the SRB-CA, see section 4.2.1.

The **Public Point** shall contain the public point of the ephemeral ERCA key pair used for key agreement, see section 4.2.3. The ERCA converts the public point to an octet string as specified in BSI Technical Guideline TR-03111 using the uncompressed encoding format.

The **Encrypted symmetric key** data element shall contain the output of step 4 in section 4.2.3.

The MAC data element shall contain the output of step 5 in section 4.2.3.

After successful generation of the key distribution message, the ERCA securely destroys its ephemeral private key for key agreement in the HSM, as well as the encryption key KENC and the MAC-ing key K_{MAC}. The key distribution message is returned to the MSCA that issued the KDR.

4.2.5 Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages, CD-R should be used:

- The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA accepts and dispatches key distribution requests and key distribution messages as e-mail attachments.

The SRB-CA shall write three copies of each key distribution request to the transport medium for transport to the ERCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

The ERCA writes three copies of each key distribution message to the transport medium for return to the SRB-CA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

Each KDR and KDM shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS. Another paper copy of the data shall be held by the ERCA or the SRB-CA, respectively.

For both KDRs and KDMs, the transport media and the printouts shall be handed over between an ERCA employee and the SRB-CA courier in the JRC controlled area.

4.2.6 Master Key Acceptance

The courier signs for receipt of the key distribution message at the ERCA premises. Upon reception of the key distribution message at the MSCA premises, the SRB-CA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with Table 3
- the message is genuine. The SRB-CA shall do this by contacting the ERCA as described in the ER-CA CPS and verifying that the MAC in the received KDM matches the MAC in the KDM sent by the ERCA;
- the master key type and version in the message matches the requested type and version;
- the public point specified in the message is on the curve specified by the key distribution request sent by the SRB-CA to the ERCA.

If any of these checks fail, the SRB-CA shall abort the process and contact the ERCA. If all of these checks succeed, the SRB-CA shall

- use the ECKA-DH algorithm to derive a shared point (Kx, Ky), as described in step 3 in section 4.2.3, using the SRB-CA's ephemeral private key indicated by the key identifier in the message and the ERCA's ephemeral public key. The MSCA shall verify that the shared point is not the infinity point; if it is, the SRB-CA shall abort the process and contact the ERCA. Else, the SRB-CA shall form the shared secret K by converting Kx to an octet string as specified in BSI Technical Guideline TR-03111;
- derive the keys KENC and KMAC as described in step 4 in section 4.2.3;
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3. If this verification fails, the MSCA shall abort the process and contact the ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3. The SRB-CA shall verify that the padding of the decrypted key, if any, is correct. If this verification fails, the SRB-CA shall abort the process and contact the ERCA.

Any operations with the ephemeral private key, with the shared secret and with the derived keys KENC and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2.

After successful recovery of the master key, or when the key distribution process is aborted and no KDM renewal (see section 4.2.8) is initiated, the SRB-CA shall securely destroy its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

4.2.7 Master Key Usage

The SRB-CA shall use any received master key in accordance to section 6.2.

4.2.8 KDM Renewal

KDM renewal means the issuance of a copy of an existing KDM to SRB-CA without changing the ephemeral public key or any other information in the KDM.

KDM renewal may take place only if the original transport media received at the MSCA is damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the SRB-NA and the ERCA. Subsequent to this report, the SRB-CA may send a KDM renewal request to the ERCA, referring to the original key distribution request. This procedure is described in the ERCA CPS. The ERCA shall only accept KDM renewal request endorsed by the SRB-NA which approved the SRB-CA. Note: In case the SRB-CA needs to send a request to re-distribute a master key that was already successfully distributed to the SRB-CA, it shall generate a new key distribution request, using a newly generated ephemeral key pair. Such a request may lead the ERCA to initiate an investigation of the possibility of key compromise.

4.2.9 Master Key Re-key

In case the ERCA has generated a new version of a master key, as specified in Appendix 11 sections 9.2.1.2 and 9.2.2.2, the availability of a new key is published on the ERCA website, together with its version number and length.

To receive the new version, the SRB-CA shall submit a new KDR. Requesting a new master key shall take place in a timely manner so that the key (or derived keys or encrypted data for motion sensors) can be placed in time in newly issued components.

Key application, processing, distribution and acceptance are the same as for the initial key. Component manufacturers and card personalizers shall be informed immediately as further described in the SRB-CA practice statement.

4.2.10 Symmetric Key Compromise Notification

If SRB-CA detects or is notified of the compromise or suspected compromise of a symmetric master key, SRB-CA shall notify this to the ERCA and the SRB-NA without unnecessary delay and at least within 8 hours of detection. In their notification, the SRB-CA shall indicate the circumstances under which the compromise occurred. Any follow-up investigation and potential action by the SRB-NA and/or SRB-CA shall be performed as indicated in the NA certificate policy. The outcome of the SRB-NA investigation shall be reported to the ERCA.

If the ERCA detects or is notified of the compromise or suspected compromise of a symmetric master key, the ERCA shall notify the European Authority without unnecessary delay and at least within 8 hours of detection. The European Authority shall act accordingly. The ERCA shall handle the incident according to a defined security incident handling procedure.

4.2.11 Master Key Status Service

The status of symmetric master keys shall be retrievable online from https://dtc.jrc.ec.europa.eu/. The ERCA shall maintain the integrity of the status information.

Master key status information published in the ERCA repository shall be updated on the first working day of each week.

The availability of the website mentioned above shall be guaranteed during normal working hours.

4.2.12 End of Subscription

Subscription for the ERCA 's key distribution services ends when an NA decides for NA termination. Such a change is notified to the ERCA by the NA as a change to the national policy.

In the case of subscription ending, the MSCA shall securely destroy all copies of any symmetric master key in its possession.

4.2.13 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that symmetric master keys shall not be exported to or stored in any system apart from the ERCA and SRB-CA production and fallback systems.

4.3 Tachograph Card Certificate Application and Issuance

More details on application and issuance of Tachograph card certificates are provided in the SRB-CA documentation. These details will be provided to registered card personalizers.

4.3.1 Certificate Application

The SRB-CA only issues certificates if a proper certificate application is presented to the responsible authority and if all the requirements of regulation (EC) 165/2014 and of all other associated legal provisions and agreements have been adhered to at the time of applying.

The SRB-CA shall only accept certificate applications for tachograph cards with a valid type approval as described in Annex IC (chapter 8).

For each tachograph card one unique ECC key pair, designated as Card_MA and used for mutual authentication, shall be generated. A second unique ECC key pair, designated as Card_Sign (used for signing of data), shall additionally be generated for each driver card and each workshop card. This task may be handled by card manufacturers or card personalizers, as described in Annex IC Appendix 11 (section 9.1.5). Whenever a card key pair is generated, the party generating the key shall send the public key to the SRB-CA in order to obtain a corresponding card certificate signed by the SRB-CA. The private key shall be used only by the tachograph card. Key certification requests that rely on transportation of private keys are not allowed.

4.3.2 Certificate Requests

Certificate requests are collected inside a request package. The packages are signed using the private key of a dedicated RA chip card as described in the SRB-CA CPS.

Data Object	Length	Format	Data
certificateRequestID	8 Byte	CertificateRequestID	Request ID
cardNumber	16 Byte	CardNumber	Card number
equipmentType	1 Byte	INTEGER	Equipment type: - Driver card: '0x01' - Workshop card: '0x02' - Control card: '0x03' - Company cards: '0x04' - Driver card signature: '0x11' - Workshop Card Signature: '0x12'
tachographApplicationID	6 Byte	OCTET STRING	Hard coded value: 'FF 53 4D 52 44 54' („SMRDT")
PK_DP	var	Object Identifier	Domain Parameter; references the standardized domain parameters to be used with the public key in the certificate. It shall contain one of the object identifiers speci fied in table 1 of Appendix 11, Annex IC
PK_PP data in plain format Table 4 Tachograph Card Certificate Request Data	var	OCTET STRING	Public Point; Elliptic curve public points shall be converted to octet strings as specified in (BSI Technical Guideline TR03111, Elliptic Curve Cryptography, V.2.0). The uncompressed encoding format shall be used (Annex IC, Appendix 11, CSM_143)
signature	var	OCTET STRING	ECC Certificate Request Signature; ECDSA Signature created over the certificate request data in plain format

Table 4 Tachograph Card Certificate Request Data

The **signature** is created over all data objects (in the specified order) except "cardNumber". The signature algorithm shall be ECDSA, as specified in FIPS PUB 186-4, using the hashing algorithm linked to the key size of the signing authority. The signature format shall be plain, as specified in BSI Technical Guideline TR-03111.

4.3.3 Certificate Issuance

The SRB-CA shall ensure within its authority, that a proper registration with the responsible authorities takes place before issuing of a certificate to the SRB-CP or card manufacturer.

If key generation takes place outside the SRB-CA, the SRB-CA shall only issue a certificate to the SRB-CP or card manufacturer if proof is made by a pre-agreed procedure that they are in possession of the corresponding private key. At this time the private key must not leave the secured environment of key generation. The SRB-CA shall also ensure that a certificate request package originating from the SRB-CP or a card manufacturer is complete, accurate, and duly authorized. The SRB-CA shall only issue or sign a card certificate if this is the case.

Checks for correctness, completeness and authorization shall only be performed in an automated way by the SRB-CA system as described in the SRB-CA CPS. The key component for authorization hereby is the RA chip card.

The SRB-CA shall only issue a certificate to a VU manufacturer if the manufacturer resides in the European Union. This doesn't refer to subsidiaries or production sites of the manufacturer.

According to Appendix 11 the validity period of a CardMA certificate shall be as follows:

- For driver cards: 5 years
- For company cards: 5 years
- For control cards: 2 years
- For workshop cards: 1 year

The validity period of a Card_Sign certificate shall be as follows:

- For driver cards: 5 years and 1 month
- For workshop cards: 1 year and 1 month

The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate. It shall be the date of issuance of the certificate by the SRB-CA.

The CardMA and CardSign certificates of a given driver card or workshop card shall have the same Certificate Effective Date.

Usage time of Card_MA.SK and Card_Sign.SK shall be the same as the validity period of the corresponding certificate.

The format of the Card_MA and CardSign certificates can be found in Section 72.

4.3.4 Certificate Acceptance

The SRB-CP or a card manufacturer shall only accept the certificate if it matches the associated certificate request and if the certificate can be validated against the SRB-CA's MSCACard certificate containing the MSCA_Card.PK.

4.3.5 Key Pair and Certificate Usage

- The SRB-CP or a card manufacturer shall choose the strength of a card key pair equal to the strength of the SRB-CA key pair used to sign the corresponding card certificate.

- A tachograph card shall use its Card_MA key pair, consisting of private key Card_MA.SK and public key CardMA.PK, exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in Annex IC, Appendix 11.
- A driver card or workshop card shall use the private key CardSign. SK of its CardSign key pair exclusively to sign downloaded data files, as specified in Appendix 11. The corresponding public key CardSign. PK shall be used exclusively to verify signatures created by the card.
- Key pairs, symmetric keys and pin numbers shall be generated and maintained in a trustworthy dedicated device which:
    - is certified to EAL 4 or higher in accordance with ISO/IEC 15408 using a suitable Protection Profile; or
    - meets the requirements identified in ISO/IEC 19790 level 3; or
    - meets the requirements identified in FIPS PUB 140-2 level 3.

The most common implementation of such a trustworthy dedicated device for use in a PKI system is a Hardware Security Module (HSM).

- Private key operations and symmetric key operations shall take place internally in the HSM where the keys used are stored.
- The private keys and symmetric keys shall only be used within a physically secure environment by personnel in trusted roles under at least dual control. Private keys and symmetric keys shall not be processed outside the HSM without adequate encryption. All events of private key usage and symmetric key usage shall be logged.
- The key pairs and corresponding certificates of a given tachograph card shall not be replaced or renewed once the card has been issued.
- When issued, tachograph cards shall contain the following cryptographic keys and certificates:
    - The Card_MA private key and corresponding certificate
    - For driver cards and workshop cards additionally: The Card_Sign private key and corresponding certificate
    - The MSCACard certificate containing the MSCACard.PK public key to be used for verification of the Card_MA certificate and Card_Sign certificate
    - The EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_Card certificate
    - The EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the MSCACard certificate, if existing.
    - The link certificate linking these two EUR certificates, if existing
    - Symmetric master keys KM_{-WC} and KM_{-DSRC} for workshop cards
    - Symmetric master key KM_{-DSRC} for control cards
- In addition to the above-mentioned cryptographic keys and certificates, tachograph cards shall also contain the keys and certificates specified in

Annex IC, Appendix 11, Part A, allowing these cards to interact with first-generation VUs.

4.3.6 Certificate Renewal

Certificate renewal, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.3.7 Certificate Re-key

Certificate re-key is not allowed. New tachograph cards shall be issued when a certificate has expired, and the usage period of the key pair has also expired.

4.3.8 Certificate Modification

Certificate modification is not allowed.

4.3.9 Certificate Revocation and Suspension

Revocation of Tachograph card certificates by the SRB-CA is not intended and revocation requests shall not be accepted and processed by the SRB-CA.

4.3.10 Certificate Status Services

Certificate status information for all issued Tachograph card certificates is maintained by the SRB-CA. This information shall not be published, but will be made available to parties having a legitimate interest upon request.

4.3.11 End of Subscription

Subscription for the SRB-CA's certification service ends when the card personalizer or card manufacturer decides for service termination. In this case all issued tachograph card certificates are allowed to expire. The card personalizer or card manufacturer notifies service termination to the SRB-NA and the SRB-CA. The SRB-NA informs the SRB-CIA's about service termination and subsequent card personalizers or card manufacturers.

4.3.12 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that the private keys Card_MA.SK and Card_Sign.SK shall not be exported to or stored in any place apart from the associated tachograph card.

4.4 Vehicle Unit (VU) Certificate Application and Issuance

Not applicable.

4.5 External GNSS Facility (EGF) Certificate Application and Issuance

Not applicable.

4.6 Symmetric Master Key VU Part ($K_{M\text{-}VU}$), Workshop Part ($K_{M\text{-}WC}$) and DSRC Master Key (K_{MDSRC}) Application and Distribution

More details on application and distribution of symmetric keys are provided in the SRB-CA documentation. These details will be provided to registered component manufacturers and card personalizers.

4.6.1 Key Distribution Requests

A formal Key distribution request (KDR) by equipment manufacturers or card personalizers is not necessary. If new symmetric keys have to be distributed, the registered contact person with access to a valid RA-card (as further specified in the SRB-CA's Practice Statement) will be contacted by the SRB-CA (usually by phone) for further coordination

4.6.2 Key Distribution Messages

Equipment manufacturers and card personalizers receive a key distribution message (KDM) as DER-encoded ASN. 1 data structure based on the encoding rules specified in ISO/IEC 8825-1 as binary file of variable length:

Data Object	**Tag**	**Length**	**Data**	**Description**
KDM	'A1'	var		Key Distribution Message
CID	'5A'	18 Byte	OCTET STRING	SRB-CA card number of related RA-card
MRA	'83'	8 Byte		Message Recipient Authorization
tacho-graphApplicati-onlD		6 Byte	,FF 53 4D 52 44 54'	The 6 most significant bytes of the application identifier (AID)
mastert er-KeyTyp e		1 Byte	$K_{M\text{-}WC}$ '27' $K_{M\text{-}VU}$: '67' $K_{M\text{-}SRC}$:09	Requested type of master key (based on equipment type definitions)
keyVers on-Number		1 Byte		Version number of requested key, INTEGER (0...255)
EAK	'5F 52'	var	OCTET STRING	Encrypted LKM with symmetric master key, padding PKCS#1, ECB mode (1)
S	'5F 37'	var	OCTET STRING	Signature of RA-CA over the hash value of the master key MK enclosed in the LKM (2)

Table 7 Structure of KDM for symmetric key distribution (Gen. 2) to equipment manufacturers and card personalizers

Comments:

(1) The below described Labeled Key Message (LKM) is encrypted with the public RSA key of the RA partner card.

(2) The signature of the master key MK is done by the RA-CA (1024 Bit RSA key, SHA1 hash value).

LKM structure

Data Object	Tag	Length	Data	Description
LKM var	'7F 24'	var		Labeled Key Message
CID	'5A'	18 Byte	OCTET STRING	SRB-CA card number of related RA-card
MRA	'83'	8 Byte		Message Recipient Authorization
tacho-graphAppli-cationID		6 Byte	,FF 53 4D 52 44 54'	The 6 most significant bytes of the application identifier (AID)
masterKeyType		1 Byte	KM-WC: '27' KM-VU: '67' KM-DSRC: '09	Requested type of master key (based on equipment type definitions)
keyVersion-Num-ber		1 Byte		Version number of requested key, INTEGER (0...255)
MK	'7F 51'	var		Master key (16, 24 or 32 Byte)

Table 8 Structure of LKM for symmetric key distribution

4.6.3 Issuance of Symmetric Master Keys

The SRB-CA shall ensure within its authority, that a proper registration with the responsible authority takes place before issuing symmetric master keys to equipment manufacturers or card personalizers. The SRB-CA shall only issue symmetric master keys to equipment manufacturers or card personalizers that reside in the European Union. This doesn't refer to subsidiaries or production sites of the equipment manufacturer or card personalizer.

4.6.4 Exchange of Requests and Responses

- For transportation of key distribution messages, CD-R media or USB flash drive (USB memory stick) should be used.
- The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).
- The USB flash drive shall use the USB mass storage device class.
- Other transport methods may be used after prior consent of the SRB-CA. For testing purposes (with test keys only), the SRB-CA shall dispatch key distribution messages as e-mail attachments.
- The SRB-CA shall write one copy of each key distribution message to the transport medium for return to the equipment manufacturer or card personalizer. This copy shall be in binary (.bin file) format.
- The transport media shall be handed over between a SRB-CA employee and the courier in the SRB-CA controlled area.

4.6.5 Key Acceptance

- The courier signs for receipt of the key distribution message at the SRB-CA premises. Upon reception of the key distribution message at the equipment manufacturers or card personalizer's premises, the partner shall check that:
  - o the transport media is readable; i.e. not damaged or corrupted;
  - o the format of the message complies with the structure described in 4.6.2;
  - o the symmetric key type and version in the message matches the requested type and version.
- If all of these checks succeed, the partner shall decrypt the symmetric key as specified in 4.6.2 using the corresponding RA card.
- Decryption of the symmetric key shall only take place in an HSM complying with the requirements in section 6.2.

4.6.6 Key Usage

Equipment manufacturers or card personalizers shall use any received symmetric key in accordance to section 6.2.

4.6.7 KDM Renewal

KDM renewal, i.e. the issuance of a copy of an existing KDM to an equipment manufacturer or card personalizer, is not allowed. In case the original transport media received by the equipment manufacturer or card personalizer is damaged or corrupted, a new KDM must be generated.

4.6.8 Key Re-key

In case the ERCA has generated a new version of a symmetric master key as specified in Appendix 11 sections 9.2.1.2 and 9.2.2.2, the availability of a new symmetric key shall be communicated to the equipment manufacturers or card personalizers by the SRB-CA for further coordination. Key application, processing, distribution and acceptance are the same as for the initial key. Distributing new symmetric keys shall take place in a timely manner so that the key (or derived keys or encrypted data for motion sensors) can be placed in time in newly issued components.

4.6.9 Symmetric Key Compromise Notification

If the component manufacturer or card personalizer detects or is notified of the compromise or suspected compromise of a symmetric key, the component manufacturer or card personalizer shall notify this to the SRB-CA and the SRB-NA without unnecessary delay and at least within 8 hours of detection. In their notification, the component manufacturers or card personalizers shall indicate the circumstances under which the compromise occurred. The component manufacturer or card personalizer shall handle the incident according to a defined security incident handling procedure. Following the incident, the results of the follow-up investigation, initial and potential actions shall be reported to the SRB-CA and the SRB-NA, for the first time not later than one week after the incident was detected.

In addition to immediate actions taken by the component manufacturer or card personalizer, SRB-CA and SRB-NA check and agree on appropriate actions, which may include the temporary or final stop of services offered by the SRB-CA to the affected component manufacturer or card personalizer. All actions taken by SRB-CA

and the SRB-NA will be coordinated with the ERCA and the incident will be reported as soon as possible but not later than 8 hours after detection or notification.

If a security incident takes place in the SRB-CA, the SRB-CA will act as described above. SRB-NA, ERCA and potentially affected component manufacturers or card personalizers will be informed immediately and not later than 8 hours after the incident is detected.

Symmetric key compromise is considered a severe security incident, which results in an extraordinary audit according to 8.1, which focuses on the actions related to the incident.

4.6.10 Key Status Service

No status service for symmetric keys will be published or especially maintained by the SRB-CA.

4.6.11 End of Subscription

Subscription for key distribution services ends when an equipment manufacturer or card personalizers decides for termination of his service. Such a change is notified to the SRB-CA by the equipment manufacturer or card personalizers.

In the case of subscription ending, the equipment manufacturer or card personalizers shall securely destroy all copies of any symmetric key in its possession.

4.6.12 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that symmetric keys shall not be exported to or stored in any system apart from the systems of the equipment manufacturers or card personalizers.

4.7 SRB-CA Encryption Services for Motion Sensor Pairing Keys and Serial Numbers and for Generation of VU-specific symmetric DSRC-Keys $K\_VU_{DSRC}\_ENC$ and $K\_VU_{DSRC}\_MAC$

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

- The key and certificate generation services of the SRB-CA and the corresponding services of component manufacturers and card personalizers shall be housed in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorized access, damage, and interference. This area shall be monitored by guards and security alarms must be established.
- Power supply and air conditioning for the SRB-CA systems must be appropriate and redundancy shall be established.
- SRB-CAs, component manufacturers and card personalizers systems and storage media used to store confidential information, such as hard disks, smart cards and HSMs, shall be protected against unauthorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Backup and installation media shall be stored in a separate location that is physically secured and protected against unauthorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Procedures for the disposal of waste shall be implemented to avoid unauthorized use, access, or disclosure of confidential data.
- An off-site facility for storage of SRB-CA critical data and data needed for emergency recovery shall be implemented.

5.2 Procedural Controls

- Procedural controls shall be implemented by the SRB-CA, component manufacturers and card personalizers to ensure secure operations. In particular separation of duties shall be enforced by implementing multiple-person control for critical tasks.
- Access to the SRB-CA systems and the corresponding systems of component manufacturers and card personalizers shall be limited to individuals who are properly authorized and, on a need-to-know basis only. In particular, the following access control measures shall be in place:
    - Confidential data shall be protected to safeguard data integrity and confidentiality when stored;
    - Confidential data shall be protected to safeguard data integrity and confidentiality when exchanged over unsecure networks;
    - Confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data, using a safe method acknowledged by the BSI.
    - The SRB-CA systems and corresponding systems of component manufacturers and card personalizers shall ensure effective user administration and access management;
    - The SRB-CA systems and corresponding systems of component manufacturers and card personalizers shall ensure that access to

information and application system functions is restricted to authorized staff and provide sufficient computer security controls for the separation of trusted roles. Particularly, the use of system utility programs shall be restricted and tightly controlled. Access shall be restricted, only allowing access to resources as necessary for carrying out the role(s) allocated to a user;

- SRB-CA's and related component manufacturers and card personalizers personnel shall be identified and authenticated before using the SRB-CA systems or the corresponding systems of component manufacturers and card personalizers.
- SRB-CA's and component manufacturers and card personalizer's personnel shall be accountable for their activities, which shall be logged in event logs as described in section 5.4;

- The SRB-CA, component manufacturers and card personalizers shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. They shall ensure that the ISMS policies address personnel training, clearances and roles. The ISMS implementation should conform to the requirements described in ISO 27001.

5.3 Personnel Controls

- The SRB-CA responsibilities may be outsourced to a specialized company, or personnel from contractors may be hired to carry out the SRB-CA responsibilities.
- All personnel involved with the SRB-CA or related personnel of component manufacturers and card personalizers shall be properly trained and shall possess the expert knowledge, experience and qualifications necessary for the services offered and appropriate to the job function. This pertains to personnel employed directly, personnel from a specialized company to which tasks have been outsourced or personnel from contractors.
- Personnel training shall be managed according to a training plan described in the respective CPS or security concept.
- Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the CPS or security concept.
- Trusted roles, on which the security of the operation is dependent, shall be clearly identified in the respective CPS or security concept. These roles and the associated responsibilities shall be documented in a role concept or comparable document. This role concept shall be defined from the viewpoint of separation of duties and least privilege. No single person shall be authorized to simultaneously perform more than one of the trusted roles.

5.4 Audit Logging Procedures

All significant security events in the SRB-CA software or related software of component manufacturers and card personalizers shall be automatically time-stamped and recorded in the system log files. This includes at least the following:

- Successful and failed attempts to create, update, remove or retrieve status information about accounts of personnel, or to set or revoke the privileges of an account;

- Successful and failed attempts to set or change an authentication method (e.g. password, biometric, cryptographic certificate) associated to a personal account;
- Successful and failed attempts to log-in and log-out on an account;
- Successful and failed attempts to change the software configuration;
- Software starts and stops;
- Software updates;
- System start-up and shut-down;
- Successful and failed attempts to add or remove an entity from the register of subscribers to which the SRB-CA currently provides key certification services, or to change any details for any of the subscribers, or to retrieve information from the register;
- Successful and failed attempts to process a certificate signing request or a key distribution request;
- Successful and failed attempts to sign a certificate or generate a key distribution message;
- Successful and failed interactions with the database(s) containing data on (the status of) issued certificates, including connection attempts and read, write and update or removal operations;
- Successful and failed attempts to connect to or disconnect from an HSM.
- Successful and failed attempts to authenticate a user to an HSM.
- Successful and failed attempts to generate or destroy a key pair or a symmetric key inside an HSM;
- Successful and failed attempts to import or export a key to or from an HSM;
- Successful and failed attempts to change the life cycle state of any key pair or symmetric key;
- Successful and failed attempts to use a private key or symmetric key inside an HSM for any purpose.

In order to be able to investigate security incidents, where possible the system log shall include information allowing the identification of the person or account that has performed the system tasks. The integrity of system event logs shall be maintained and shall be protected from unauthorized inspection, modification, deletion or destruction. System events logs shall be backed-up and stored internally.

5.5 Records Archival

- An overview of the events which shall be archived shall be described in internal procedures and shall be in accordance with relevant rules and regulations. The SRB-CA, component manufacturers and card personalizers shall implement appropriate record archival procedures. Procedures shall be in place to ensure integrity, authenticity and confidentiality of the records.

- For all archived information, archival periods shall be indefinite.

- Measures shall be taken to assure that the record archive is stored in such a way that loss is reasonably excluded.
- The events mentioned in section 5.4 shall be inspected periodically for integrity. These inspections shall take place at least annually.

5.6 Key Changeover

- SRB-CA shall generate new SRB-CA key pairs as needed. After SRB-CA has generated a new key pair, it shall submit a certificate re-key request as described in the appropriate section of the ERCA policy and distribute the keys to the component personalizers SRB-CP as described in the re-keying sections in chapter 4 of this policy.
- The SRB-CA shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in this certificate policy.

5.7 Compromise and Disaster Recovery

The SRB-CA, component manufacturers and card personalizers shall define security incident and compromise handling procedures in a Security Incident Handling Procedure manual, which shall be issued to administrators and auditors.

The SRB-CA, component manufacturers and card personalizers shall maintain a Business Continuity Plan detailing how they will maintain their services in the event of an incident that affects normal operations. On detection of an incident, operations shall be suspended until the level of compromise has been established. The SRB-CA, component manufacturers and card personalizers shall furthermore assume that technological progress will render their IT systems obsolete over time. Measures to manage obsolescence shall be defined in the Business Continuity Plan.

Back-up and recovery procedures for all relevant data shall be described in a Back-up and Recovery Plan.

The following incidents are considered to be disasters:

- compromise or theft of a private key (SRB-CA_Card.SK,) and / or symmetric master key ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$);
- loss of a private key (SRB-CA_Card. SK,) and / or a symmetric master key ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$)
- IT hardware failure.

In the event of compromise or theft of a SRB-CA private key used to sign the public key certificates of tachograph cards (SRB-CA_Card. SK) a), the SRB-CA shall immediately inform the SRB-NA, the SRB-CIA, the affected component personalizers SRB-CP and the ERCA. All affected parties shall take appropriate measures within a reasonable time period.

In the event of compromise or theft of one or more of the symmetric master keys stored by the SRB-CA, the SRB-CA shall immediately inform the SRB-NA, the ERCA and the affected component personalizers. All affected parties shall take appropriate measures within a reasonable period of time.

There is effectively no recovery from a loss of the SRB-CA private keys or of the symmetric master keys. Loss shall therefore be prevented by using multiple backup copies of the respective keys and master keys, subjected to periodic controls.

Protection against IT hardware failures shall be provided by redundancy, i.e. availability of duplicate IT hardware.

These mechanisms shall not depend on the ERCA response times.

5.8 Service Termination

In the event of termination of SRB-CA activity by the appointed organization, the SRB-NA shall notify the EA and the ERCA of this and optionally inform the EA and ERCA about the newly appointed SRB-CA. The SRB-NA shall ensure that at least one SRB-CA is operational at all times.

If a component manufacturer terminates its activities, the SRB-CA shall be notified. The SRB-CA then notifies the SRB-NA and optionally the SRB-NA informs the EA and ERCA.

In the event of service termination of a card personalizer the SRB-CA, SRB-NA and the CIA's shall be informed of this and the SRB-NA optionally informs the EA and ERCA. The SRB-NA shall ensure that at least one card personalizer is operational at all times. The SRB-NA informs the CIA's, EA and ERCA about the newly appointed card personalizer.

6 Technical Security Controls

6.1 Key pair generation and installation

- The SRB-CA, component manufacturers and card personalizers shall generate private keys in accordance with Annex IC Appendix 11.
- Generation and insertion of key pairs and master keys shall be undertaken in a physically secured environment by personnel in trusted roles under at least dual person control. The key generation ceremony shall be documented.
- The SRB-CA shall have available a Test SRB-CA system for interoperability test purposes, according to the Regulation. The Test SRB-CA system shall be a separate system and shall have its own SRB-CA private keys and symmetric master keys. The Test SRB-CA system shall be able to request the signing of test certificates and the distribution of symmetric test keys using the processes described in this document and the ERCA Policy. The Test SRB-CA shall also be able to sign test equipment certificates on request of component personalizers and to distribute symmetric test keys and encrypted data for motion sensors to component personalizers.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The SRB-CA, component manufacturers and card personalizers shall maintain the confidentiality, integrity, and availability of the private keys and the symmetric keys as described in this section.

The private keys and symmetric keys shall be generated and used in a trustworthy dedicated device which:

- is certified to EAL 4 or higher in accordance with ISO/IEC 15408 using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3; or
- offers an equivalent level of security according to an equivalent national or internationally recognized evaluation criteria for IT security.

The most common implementation of such a trustworthy dedicated device for use in a PKI system is a Hardware Security Module (HSM). Other implementations using different devices are possible as well, as long as the adopted devices satisfy one of the security requirements listed above. In addition, apart from these security requirements, this SRB-NA certificate policy contains various functional requirements for the trustworthy dedicated device used in the SRB-CA system. Please note that in case a different device is used in place of an HSM, all such functional requirements have to be satisfied as well. The term "HSM" is used in this document as an abbreviation for the here mentioned requirements.

Private key operations and symmetric key operations shall take place internally in the HSM where the keys used are stored.

The SRB-CA, component manufacturers and card personalizers' private keys and symmetric keys shall only be used within a physically secure environment by personnel in trusted roles under at least dual control. All events of private key usage and symmetric master key usage shall be logged.

The SRB-CA, component manufacturers and card personalizers' private keys and the symmetric keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual person control in a physically secured environment.

Back-up copies of the SRB-CA, component manufacturers and card personalizers' private keys and the symmetric keys shall be subject to the same level of security controls as the keys in use.

One back-up copy of each SRB-CA private key and of each master key shall be maintained off-site.

Private key import and export shall only take place for backup and retrieval purposes.

Symmetric key import and export is allowed for backup and retrieval. For the SRB-CA, export of and KM-WC and the VU-specific keys for DSRC is allowed in encrypted form in response to a valid key distribution request from a component personalizer by personnel in trusted roles under at least dual person control.

Master key import and export for any other reason is forbidden.

At the end of the life cycle of a SRB-CA private key or of a symmetric master key (as specified in the SRB-CA CPS), all copies of the key shall be destroyed such that it cannot be retrieved.

Private keys and symmetric keys shall be deactivated and destroyed if compromise is suspected. The keys shall be destroyed after the compromise has been investigated and the decision has been taken to deactivate the key.

Destroying of private keys and master keys shall be done by using the function of the HSM for key destroying. Also, the back-up copies of compromised keys shall be destroyed.

6.3 Other Aspects of Key Pair Management

The SRB-CA public key certificates and hence the public keys shall be archived indefinitely.

The validity periods of all SRB-CA certificates shall comply with Annex IC Appendix 1.

In accordance with Annex IC Appendix 11, the private key usage period of SRB-CA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate. The SRB-CA shall not use a private key after the private key usage period is over.

6.4 Activation Data

SRB-CA private keys and/or symmetric master keys stored in an HSM shall be activated for use if all of the multiple persons controlling the key have authenticated themselves towards the HSM. Authentication shall take place by using proper means (e.g. passphrases, authentication tokens).

The duration of an authentication session shall not be unlimited.

For activation of the SRB-CA software itself, user authentication shall take place using proper means (e.g. by a passphrase).

6.5 Computer Security Controls

The SRB-CA, component manufacturers and card personalizers shall specify and approve procedures and specific technical security measures for managing its computer systems. These procedures shall guarantee that the required security level is always met. The procedures and technical security measures shall be described in internal documentations and/or security concepts. Computer systems shall be arranged and managed conforming to these procedures, the procedures specified in the security concepts and best practice procedures for trust centers and for trustworthy computing.

6.6 Life Cycle Security Controls

The SRB-CA, component manufacturers and card personalizers shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built into their systems.

A separation between Acceptance (or Pre-Production) and Production systems shall be maintained. Change procedures and security management procedures shall guarantee that the required security level is maintained in the Production system.

Change control procedures shall be documented and used for releases, modifications and (emergency) software fixes for any operational software.

6.7 Network Security Controls

The SRB-CA, component manufacturers and card personalizers shall devise and implement its network architecture in such a way that access from the internet to their internal network domain and from the internal network domain to the Certification Authority systems and related systems of component manufacturers and card personalizers can be effectively controlled.

6.8 Time-Stamping

The time and date of an event shall be included in every audit trail entry. The SRB-CA CPS and the related documentation / CPS of component manufacturers and card personalizers shall describe how time is synchronized and verified.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile

All certificates shall have the profile specified in Annex IC, Appendix 11 and Appendix 1:

Data Object	Req	Field ID	Tag	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	m	C	'7F 21'	var	
Certificate Body	m	B	'7F 4E'	var	
Certificate Profile Identifier	m	CPI	'5F 29'	'01'	INTEGER (0...255)
Certification Authority Reference	m	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation	m	CHA	'5F 4C'	'07'	Certificate Holder Authorisation
Public Key	m	PK	'7F 49'	var	
Standardised Domain Parameters OID	m	DP	'06'	var	OBJECT IDENTIFIER
Public Point	m	PP	'86'	var	OCTET STRING
Certificate Holder Reference	m	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date	m	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date	m	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature	m	S	'5F 37'	var	OCTET STRING

Table 9 Certificate

The algorithm is indicated via the Standardised Domain Parameters OID as specified in Table 1 of Appendix 11, Annex 1C. The options are:

Name	Object Identifier reference	Object identifier value
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
BrainpoolP384r1	BrainpoolP384r1	1.3.36.3.3.2.8.1.1.11

Table 11 Allowed Standardized Domain Parameters OIDs

7.2 CRL Profile

No CRL shall be published. For the ERCA, the status of all certificates issued can be found on the website https://dtc.jrc.ec.europa.eu/

7.3 OCSP Profile

No OCSP shall be used.

8 Compliance Audit and other Assessments

8.1 Frequency or Circumstances of Assessment

- A full and formal audit on the SRB-CA operation and the operation of component manufacturers and card personalizers shall be performed by order of the SRB-NA. The audit shall establish whether the requirements in this certificate policy and the ERCA policy are being maintained. The SRB-NA shall perform the first audit within 12 months of the start of the operations covered by the approved SRB-NA certificate policy.
- Before the start of the operations covered by the SRB-NA certificate policy, the SRB-NA shall carry out a pre-operational assessment to obtain evidence that the organization is able to operate in conformance to the requirements in the SRB-NA certificate policy.
- If an audit finds no evidence of non-conformity, the next audit shall be performed within a period of 12 to 24 months. If an audit finds evidence of non-conformity, a follow-up audit shall be performed within 12 months to verify that the non-conformities have been solved.
- In case of a severe security incident an extraordinary audit shall be performed within 6 months after detection of the incident. Severe incidents in this context are especially the loss of integrity or confidentiality of private and/or symmetric keys. This audit shall focus on the circumstances and follow-up measures with regard to the incident. The normal audit frequency as described in 8.1 is not affected by an extraordinary audit after a security incident.
- The SRB-NA shall report the results of the audits and provide the audit reports, in English, to the ERCA. The audit reports shall define any corrective actions, including an implementation schedule, required to fulfil the SRB-NA obligations.

8.2 Identity/Qualifications of Assessor

- The audit shall be performed by an independent auditor.
- Any person selected or proposed to perform a compliance audit of the SRB-CA, component manufacturers or card personalizers shall first be approved by the SRB-NA.
- The names of the auditors which will perform the audits shall be registered. Such auditors shall comply with the following requirements:
    - Ethical behavior - trustworthiness, uniformity and confidentiality regarding their relationship to the audited parties and when handling its information and data;
    - Fair presentation - findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit;
    - Professional approach - has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in information technologies, PKI and the related technical norms and standards.

  - Good repute - a certificate of good conduct shall be provided to the SRB-NA.

- The auditor shall possess significant knowledge of, and preferably be accredited for:
  - Performance of information system security audits;
  - PKI and cryptographic technologies;
  - The operation of PKI software;
  - The relevant European Commission policies and regulations.

8.3 Assessor's Relationship to assessed Entity

- The auditor shall be independent and not connected to the SRB-CA, a component manufacturer or a card personalizer.

8.4 Topics covered by Assessment

- The audit of the SRB-CA, component manufacturers or card personalizers shall cover compliance to the ERCA policy, the SRB-NA certificate policy, the SRB-CA CPS and the CPS or similar documents from component manufacturers or card personalizers for Gen. 2 Smart Tachographs as well as associated procedures and techniques documented by the SRB-CA or component manufacturers and card personalizers.
- The subjects of the compliance audit shall be the implementation of the technical, procedural and personnel practices described in these documents. Some areas of focus for the audits shall be:
  - Identification and authentication;
  - Operational functions/services;
  - Physical, procedural and personnel security controls;
  - Technical security controls;
  - Security incident handling procedures.
- By assessment of the audit logs it shall be determined whether weaknesses are present in the security of SRB-CA or component manufacturers and card personalizers systems. Determined (possible) weaknesses shall be mitigated. The assessment and possible weaknesses shall be recorded.
- In case of an extraordinary audit triggered by a severe security incident the audit shall focus on processes and technical measures with regard to the security incident.

8.5 Actions taken as a Result of Deficiency

If deficiencies for non-conformity are discovered by the auditor, corrective actions shall be taken immediately by the SRB-CA, component manufacturers or card personalizers. After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.6 Communication of Results

The independent auditor shall report the full results of the compliance audit in Serbian and English language to the audited entity (SRB-CA, component manufacturer or card personalizer) and the SRB-NA. The SRB-NA shall send an audit report for the SRB-CA covering the relevant results of the audit to the ERCA. This shall include at least the number of deviations found and the nature of each deviation. The audit report reception date shall be published on the ERCA website.

If requested by the ERCA, the SRB-NA shall send the full results of the compliance audits of all requested entities to the ERCA.

9 Other Business and legal Matters

9.1 Fees

Fees for symmetric keys, encryption services and certificates are calculated solely based on actual costs for providing the necessary services by the SRB-CA.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

Confidential data shall comprehend:

- Personal data (e.g. from SRB-CA employees, component manufacturers or ERCA representatives);
- Private keys;
- Symmetric master keys;
- Company or manufacturing data;
- Reasons for certificate revocation;
- Audit logs (unless access is required by law, regulations, or provisions of the CP or CPS);
- Detailed documentation regarding the PKI management;
- Audit reports by internal or external auditors.

Confidential information shall not be released, unless a legal obligation exists to do so.

9.4 Privacy of Personal Information

The only personal data processed or stored in the SRB-CA system is those of ERCA, SRB-CA and component personalizer representatives.

This data shall be treated according to the General Data Protection Regulation 2016/679.

9.5 Intellectual Property Rights

The SRB-CA owns comprehensive property rights for the SRB-CA software as defined in the appropriate contracts.

9.6 Representations and Warranties

The SRB-CA shall operate according to the ERCA CP, this CP and its own CPS.

9.7 Disclaimers of Warranties

The SRB-CA disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorized source), and further disclaims any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

9.8 Limitations of Liability

The Republic of Serbia is not liable for any loss:

- of service due to war, natural disasters or other uncontrollable forces;
- incurred between the time certificate status changes and the next scheduled issuance of certificate status information;
- due to unauthorized use of certificates issued by the SRB-CA, and use of certificates beyond the prescribed use defined by this Certificate Policy and the SRB-CA Certification Practice Statement;
- caused by fraudulent or negligent use of certificates and/or certificate status information issued by the SRB-CA.

The Republic of Serbia disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon:

- any certificate issued by the SRB-CA, or its associated public/private key pair, used by a subscriber or relying party;
- any symmetric key distributed by the SRB-CA, used by a subscriber or relying party;
- any encryption service provided by the SRB-CA and used by a subscriber or relying party.

Issuance of certificates, symmetric keys and encryption services by the SRB-CA does not make the Republic of Serbia or the SRB-CA an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the Smart Tachograph key management system.

Subscribers and relying parties are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this key management system.

In addition, the SRB-CA is not an intermediary to transactions between subscribers and relying parties. Claims against the SRB-CA are limited to showing that it operated in a manner inconsistent with this certificate policy and the SRB-CA CPS.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

This SRB-NA Certificate Policy is valid from the moment the SRB-CA becomes operational. It shall be valid until further notice.

The validity of this CP ends when the SRB-CA stops operating or when the SRB-NA announces this CP is no longer valid, e.g. because a new version of the CP becomes effective.

9.11 Individual Notices and Communications with Participants

Official notices and communications with participants in the Smart Tachograph key management system shall be in written form, and subject to the registration procedures for correspondence in force within the European Commission.

Notice of severance or merger may result in changes to the scope, management and/or operation of the DCA. In such an event, this SRB-NA certificate policy and the SRB-CA CPS may require modification as well. Changes to these documents shall be made in a manner consistent with the administrative requirements stipulated in section 9.12 of this document.

9.12 Amendments

This CP is issued under responsibility of the SRB-NA. The SRB-NA may revise this CP if it deems this necessary.

The procedure for change propositions and approvals of this CP shall be as follows:

1. Comments or requests for changes to the CP shall be directed to the SRB-NA. Such communication shall include a description of the comment or requested change, a rationale, and contact information for the person submitting the comments or requesting the change.

2. The SRB-CA shall accept, accept with modifications, or reject the comment or proposed change after completion of the comment period. SRB-CA disposition of proposed changes are reviewed by the SRB-NA. Decisions with respect to the proposed changes are at the discretion of the SRB-CA and the SRB-NA.

3. A new version of this CP or anything equivalent, as any non editorial modification of the policy shall be approved by ERCA, except the change of CA/CP). A new version of this CP will be published on the SRB-NA website after approval by the ERCA.

Every change to this CP shall be accompanied by an increase in the version number of the document. The only changes that may be made to the CP and CPS with no change to the document version number are editorial or typographical corrections.

The SRB-CA may change the contact information in section 1.5 with notification to the SRB-NA and the ERCA, but without change to the document version number. All other changes to the CP shall be made according to the amendment procedure outlined in this section.

9.13 Dispute Resolution Provisions

Any dispute related to key and certificate management for the digital Tachograph system between the DCA and an organization or individual outside of the European Commission shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the European Authority.

9.14 Governing Law

Serbian and European regulations shall govern the enforceability, construction, interpretation, and validity of this SRB-NA Certificate Policy.

9.15 Compliance with Applicable Law

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 of the European Parliament and of the Council and with Commission Implementing Regulation (EU) 2016/799. In case discrepancies exist between this document and the Regulation or Implementing Regulation, the latter shall prevail.

9.16 Miscellaneous Provisions

No stipulation

9.17 Other Provisions

No Stipulation

10 References

1. Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014, Official Journal of the European Union L60
2. Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139
3. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
4. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
5. ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, version 1.1.1, 2016-02
6. ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, version 2.4.1, 2013-02
7. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0, Month year
8. Smart Tachograph - Equipment Interoperability Test Specification, JRC, version 1.0, Month year
9. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28
10. ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition, 2006-05-01
11. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 - 2014
12. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
13. CEN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services
14. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15
15. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001
16. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013

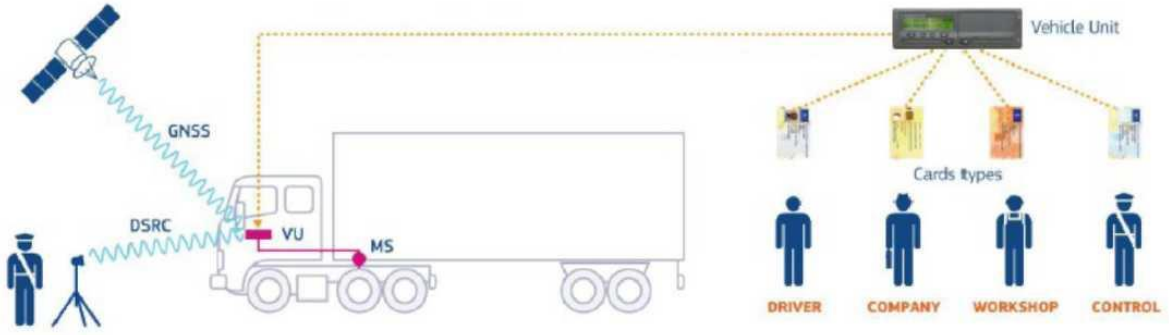
17. ISO/IEC 9797-1, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
18. National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
19. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01
20. Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission, Adopted 29/05/2009
21. Commission Decision 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission
22. Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy version 1.0 June 2018
23. Commission Implementing Regulation (EU) 2018/5002
24. Regulation (EU) 2016/679 (General Data Protection Regulation - OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018
25. Law on working hours of crews of vehicles engaged in road transport and tachographs, Official Gazette of RS, no. 96/15 and 95/18;
26. Law on Personal Data Protection, Official Gazette of RS, no. 87/18
27. Law on Electronic document, electronic identification and confidential services in the electronic business, Official Gazette of RS, no. 94/17
28. Law on Electronic Commerce, Official Gazette of RS, no. 41/09, 95/13 and 52/19

НЕЗВАНИЧАН ПРЕВОД

Република Србија

Министарство грађевинарства, саобраћаја и инфраструктуре

Политика националног тела Републике Србије за систем паметних тахографа (Политика ST-SRB-NA, V 1.1)



Слика: Јединица у возилу
Врсте картица

Возач Превозник Радионица Надзор

Историја измена

Контрола верзије	**Датум**	**Статус**
Верзија 1.0.	мај 2021. године	Почетна верзија за ERCA
Верзија 1.1.	октобар 2021. године	Исправке, укључивање напомена JRC-а и укључивање именованих SRB-CP и SRB-CA

Садржај

1 Увод

1.1 Преглед

Систем дигиталних тахографа друге генерације под називом „паметни тахографи”, уведен је Уредбом (ЕУ) број 165/2014 Европског парламента и Савета.

Анекс IB Спроведбене Уредбе Комисије (ЕУ) 2016/799 утврђује техничке захтеве за израду, испитивање, уградњу, функционисање и оправку паметних тахографа и њихових компоненти. Додатак 11. (Заједнички безбедносни механизми) Анекса IB наводи безбедносне механизме који обезбеђују:

- узајамну аутентификацију између различитих компоненти тахографског система;
- поверљивост, интегритет, аутентичност и/или непорецивост података који се преносе између различитих компоненти тахографског система или се преузимају на екстерне медијуме за складиштење података.

Део Б Додатка 11. описује како се користе криптографски системи са јавним кључем засновани на елиптичним кривама и симетрични криптографски системи засновани на AES да би се то реализовало код тахографских система друге генерације.

Инфраструктура јавног кључа (PKI) осмишљена је да подржи криптографске системе са јавним кључем, док се симетрични криптографски систем ослања на главне кључеве који морају бити уручени релевантним актерима. Успостављена је инфраструктура која се састоји од три слоја. На европском нивоу, Европско коренско сертификационо тело (ERCA) одговорно је за генерисање коренских (*root*) парова јавних и приватних кључева са одговарајућим сертификатима и симетричних главних кључева, као и за управљање тим кључевима. ERCA издаје сертификате националним сертификационим телима (SRB-CA) и дистрибуира симетричне главне кључеве сертификационим телима држава чланица (MSCA). MSCA је одговорно за издавање сертификата о уређају паметног тахографа, као и за дистрибуцију симетричних главних кључева и других података изведених из главних кључева који се уграђују у уређај паметног тахографа.

Овај документ чини политику сертификације (CP) за PKI сертификационог тела Републике Србије (SRB-CA). Он утврђује политику на нивоу националног тела (NA) за генерисање кључева, управљање кључевима и потпис сертификата за систем паметних тахографа која се заснива на политици сертификације ERCA. Да би SRB-CA издавало сертификате и/или симетричне кључеве персонализаторима компоненти SRB-CP, оно мора испуњавати захтеве који су такође утврђени у овом документу.

Овај документ прати оквир за CP описан у RFC 3647.

Усклађеност самог SRB-CA са овом политиком сертификације и инфраструктуре симетричних кључева описана је у Општим правилима рада SRB-CA (CPS SRB-CA) за систем паметних тахографа. Дигитални тахограф (систем прве генерације) и паметни тахограф (систем друге генерације) су два различита система која морају функционисати паралелно и независно. Због тога морају постојати одвојене политике NA како би се избегли проблеми када у будућности дође време да се укине дигитални тахограф и његово одговарајуће ERCA (прве генерације). Из тог разлога ће „Национална политика за систем дигиталних тахографа у Републици Србији ” остати на снази упоредо са овом политиком SRB-NA.

Кључне речи „захтева”, „мора”, „не сме”, „треба”, „не треба”, „препоручено”, „може” и „необавезно” у овом документу треба тумачити како је описано у RFC 2119.

1.2 Надлежне организације

Орган надлежан за спровођење политике SRB-NA, у даљем тексту: SRB-NA (Национално тело Републике Србије) је

Министарство грађевинарства, саобраћаја и инфраструктуре,
Сектор за друмски транспорт, путеве и безбедност саобраћаја
Немањина 22-26
11000 Београд
Република Србија

Именовано SRB-CIA је:

Агенција за безбедност саобраћаја (АБС)
Булевар Михајла Пупина 2
11000 Београд
Република Србија

Именовано SRB-CA је:

Народна банка Србије
Завод за израду новчаница и кованог новца – Топчидер
Пионирска 2
11000 Београд
Република Србија

Именовано SRB-CP је:

Народна банка Србије
Завод за израду новчаница и кованог новца – Топчидер
Пионирска 2
11000 Београд
Република Србија

SRB-CA или SRB-CP могу за делове својих процеса закључити уговоре са подизвођачима и агенцијама за пружање услуга. Коришћење агенција за пружање услуга ни на који начин не умањује целокупне одговорности SRB-CA или SRB-CP.

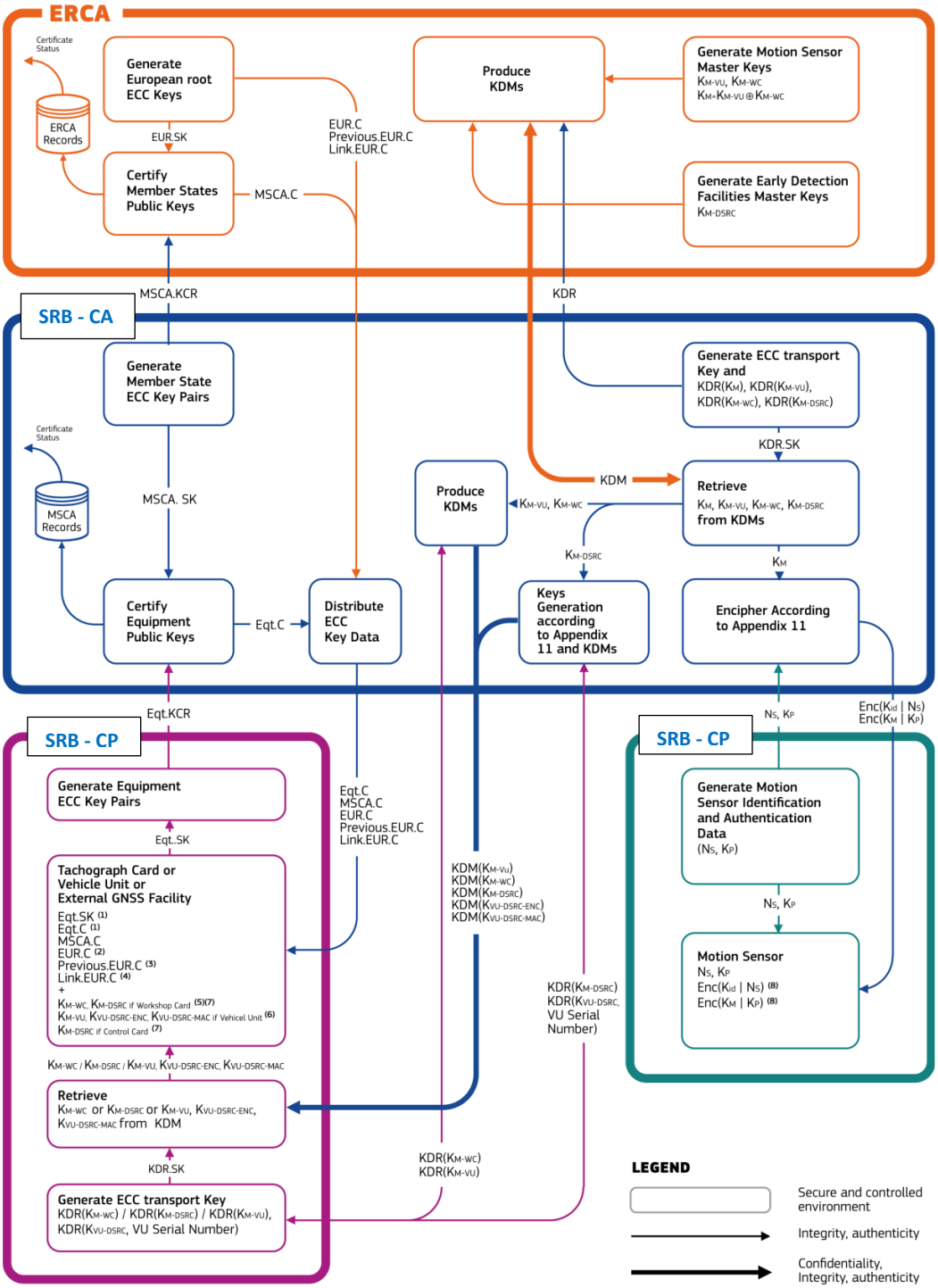
1.3 Назив документа и идентификациона ознака

Овај документ носи назив „Политика националног тела Републике Србије за систем паметних тахографа”. Ова политика сертификације нема идентификатор објекта ASN.1. Такав идентификатор није потребан јер сертификати који се користе у систему паметних тахографа не садрже упућивање на ову политику. Актуелна верзија може се наћи на почетку овог документа. **Верзију 1.1.** ове политике одобрило је ERCA (видети одељак 1.5.1) **25. новембра 2021. године. Ref. Ares(2021)7275663 – 25/11/2021.**

1.4 Учесници PKI

Учесници у PKI паметних тахографа и у инфраструктури симетричних кључева су описани су и представљени на Слици 1. Слика 1. представља и размене између учесника, односно ERCA, MSCA и персонализатора компоненти SRB-CP.

За више информација о симетричним и асиметричним кључевима поменутим у овом одељку видети Додатак 11. Део Б.



NOTES

1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Легенда:
Сигурно и контролисано окружење
Интегритет, аутентичност
Поверљивост, интегритет, аутентичност

Напомена:
1. За VU и тахографске картице постоје два сертификата и одговарајући кључеви, један за узајамну аутентификацију (MA) и један за потписивање (Sign).

2. EUR сертификат коришћен за генерисање MSCA C сертификата.
3. EUR сертификат чије важење претходи периоду важењу EUR сертификата из напомене 2, ако он постоји.
4. Сертификат о повезивању који повезује EUR сертификате из напомена 2. и 3, ако постоје.
5. Сви кључеви $K_{M\text{-}WC}$ повезани са кључевима $K_{M\text{-}VU}$ који су тренутно у оптицају морају бити уметнути.
6. Кључ $K_{M\text{-}VU}$ повезан са EUR сертификатом из напомене 2.
7. Сви кључеви $K_{M\text{-}DSRC}$ који су тренутно у оптицају морају бити уметнути.
8. NS и KP морају бити шифровани према свим кључевима K_M који су тренутно у оптицају.

Слика 1. PKI паметног тахографа и инфраструктура симетричних кључева

1.4.1 Сертификациона тела

1.4.1.1 Европско коренско сертификационо тело (ERCA)

ERCA је коренско сертификационо тело (CA) које креира и додељује сертификате јавних кључева у PKI. Оно управља следећим услугама које се односе на компоненте:

услугом регистрације, услугом генерисања сертификата, услугом дистрибуције.

ERCA генерише коренске парове кључева PKI и одговарајуће сертификате, заједно са сертификатима о повезаности да би се створио ланац поверења између различитих коренских сертификата.

ERCA је и субјект који генерише симетричне главне кључеве, тј. главни кључ сензора кретања-део јединице у возилу (VU) ($K_{M\text{-}VU}$), главни кључ сензора кретања-део картице радионице ($K_{M\text{-}WC}$) и главни кључ DSRC-а ($K_{M\text{-}DSRC}$), управља њима и на захтев их дистрибуира.

1.4.1.2 Сертификационо тело Републике Србије (SRB-CA)

SRB-CA функционише као подређено CA у односу на ERCA. Оно креира и додељује сертификате јавних кључева за уређај. У ту сврху пружа услугу регистрације, услугу генерисања сертификата и услугу дистрибуције. SRB-CA добија захтеве за сертификате од персонализатора компоненти SRB-CP и тим странама дистрибуира сертификате за издавање сертификата картица, који се називају пар кључева картице MSCA. SRB-CA захтева сертификате MSCA од ERCA због његове одговорности у погледу издавања сертификата картица. SRB-CA такође захтева од ERCA симетричне главне кључеве и $K_{M\text{-}WC}$ и $K_{M\text{-}DSRC}$ персонализатора картица.

1.4.2 Регистрациона тела

1.4.2.1 Тело за издавање картица Републике Србије (SRB-CIA)

SRB-NA задужено је да именује SRB-CIA.

SRB-CIA одговорно је за следеће:

- именује SRB-CA и SRB-CP;
- проверава да ли су сачињени сви потребни документи;
- проверава да ли су испуњени сви предуслови за издавање тахографске картице у складу са Уредбом (ЕУ) број 165/2014 Европског парламента и Савета, Анексом IB Спроведбене уредбе Комисије (ЕУ) 2016/799, свим осталим релевантним правним одредбама, политиком ERCA и овом политиком SRB-NA;
- проверава да тахографска картица није већ издата подносиоцу захтева у другој држави чланици ЕУ;

- проверава да ли је корисник сваке тахографске картице идентификован у некој фази процеса издавања картице;
- стара се о томе да се подаци из захтева правилно пренесу SRB-CP у складу са сачињеним документима и захтевима из ове политике;
- информише све кориснике о захтевима из ове политике на одговарајући начин;
- стара се о томе да се PIN картице радионице преда само доносиоцу картице радионице коме је намењен тако што се користе одвојени примаоци за картицу радионице (радионица) и PIN (именовани техничар);
- одмах обавештава SRB-NA и SRB-CA или једну од његових овлашћених агенција о свим безбедносно релевантним инцидентима.

1.4.2.2 Регистрационо тело SRB-CA

SRB-CA се у оквиру својих овлашћења стара о томе да се изврши правилна регистрација произвођача компоненти и персонализатора картица SRB-CP пре издавања сертификата, дистрибуције симетричних кључева или шифровања података о уређају. Процес регистрације детаљно је описан у CPS-у.

1.4.3 Претплатници

Једини претплатници услуге сертификације јавних кључева SRB-CA су персонализатори компоненти SRB-CP. Персонализатори компоненти SRB–CP одговорни су за персонализацију следећег:

- тахографских картица: постоје четири различите врсте тахографских картица: картице возача, картице привредног друштва, картице радионице и контролне картице.
- Картице возача и картице радионице имају два пара кључева и одговарајуће сертификате које је издало MSCA_Card, односно
    - пар кључева и сертификат за узајамну аутентификацију који се назива Card_MA;
    - пар кључева и сертификат за узајамну аутентификацију који се зове Card_MA;

Картице радионице такође садрже $K_{M\text{-}WC}$ и $K_{M\cdot DSRC}$ са дужином кључа свих могућих VU - у погледу коришћених пакета шифри.

- Картице привредног друштва и контролне картице имају пар кључева и одговарајући сертификат који издаје MSCA_Card за узајамну аутентификацију.

Картице радионице садрже и $K_{M\text{-}DSRC}$ са дужином кључа свих могућих VU - у погледу коришћених пакета шифри.

Персонализатори компоненти SRB-CP одговорни су да обезбеде да уређај има одговарајуће кључеве и сертификате.

1.4.3.1 Персонализатор српских тахографских картица (SRB-CP)

- Захтеви у погледу произвођача јединица у возилу и сензора кретања тренутно нису обухваћени овом политиком. Ова политика се у случају потребе мора прилагодити.
- обезбеђује генерисање два пара кључева картица, за узајамну аутентификацију и за потпис, који су намењени за картицу возача и картицу радионице;

- спроводи поступак подношења захтева за сертификат код SRB-CA_Card за картицу возача и картицу радионице;
- подноси захтев за K_{M-WC} и K_{M-DSRC} (само картице радионице);
- обезбеђује расположивост кључева и сертификата на картици за узајамну аутентификацију и потпис, упаривање MoS-VU и дешифровање комуникације DSRC-а, као и проверу аутентичности података (само картице радионице);
- обезбеђује генерисање парова кључева картица за узајамну аутентификацију за привредна друштва и контролне картице;
- спроводи поступак подношења захтева за сертификат код SRB-CA_Card за привредна друштва и контролне картице;
- врши пријаву K_{M-DSRC} (само контролне картице);
- обезбеђује расположивост кључева и сертификата на картици за узајамну аутентификацију и дешифровање комуникације DSRC-а, као и проверу аутентичности података (само контролне картице).

1.4.4 Трећа лица

Стране које се ослањају на услуге сертификације SRB-CA првенствено су органи Србије чији је задатак да спроводе правила и прописе у вези са временом вожње и одмора, посебно полиција Србије.

Сертификати SRB-CA користе се у оквиру система за проверу аутентичности сертификата за уређај, који се затим користе за проверу аутентичности података преузетих са јединица у возилу и картица возача. Други директни учесници су произвођачи компоненти и персонализатори, тела за издавање картица (CIA), возачи, привредна друштва и радионице.

1.5 Коришћење кључева и сертификата

SRB-CA користи своје приватне кључеве SRB-CA само за:

- потписивање захтева за потпис сертификата (видети одељак 4.1.1)
- издавање листе опозваних сертификата (CRL), ако се такав метод користи за пружање информација о статусу сертификата.

SRB-CA користи симетричне главне кључеве искључиво за извођење кључева специфичних за дату VU и шифровање података у вези са сензором кретања, како је наведено у Анексу IB, Додатак 11.

SRB-CA доставља симетричне главне кључеве, кључеве добијене из тих главних кључева или податке шифроване овим главним кључевима персонализаторима компоненти SRB-CP средствима осигураним на одговарајући начин, само у сврху за коју су кључеви и подаци намењени, како је наведено у Анексу IB, Додатак 11.

Сертификати SRB-CA_Card користе се за проверу сертификата картица које издаје SRB-CA_Card.

Сертификати Card_MA користе се за узајамну аутентификацију и усаглашавање серијских кључева између картице и VU.

Сертификати Card Sign користе се за проверу аутентичности и интегритета података преузетих са картице. Приватни кључ Card Sign може се користити само за потписивање података преузетих са картице. SRB-CA користи све важеће верзије K_M за шифровање кључева за упаривање сензора кретања (MoS) K_P и за извођење свих

важећих верзија идентификационог кључа MoS K_{ID}. SRB-CA користи све важеће верзије K_{ID} за шифровање серијских бројева MoS. $K_{M\text{-}VU}$ и $K_{M\text{-}WC}$ достављају се персонализаторима компоненти SRB-CP ради њихове инсталације у VU односно картице радионице. VU користи KM-VU заједно са одговарајућим KM-WC за генерисање правог KM током упаривања VU и MoS.

SRB-CA користи $K_{M\text{-}DSRC}$ за извођење кључева специфичних за дату VU ради обезбеђивања комуникације DSRC-а. Контролне картице и картице радионице користе $K_{M\text{-}DSRC}$ за извођење кључева DSRC-а специфичних за дату VU који су потребни за дешифровање и проверу аутентичности и интегритета комуникације DSRC-а у VU.

1.6 Примена политике

1.6.1 ERCA

Служба Европске комисије одговорна за спровођење политике сертификације на европском нивоу и за пружање услуга сертификације кључева и дистрибуције кључева државама чланицама назива се *European Root Certification Authority* (Европско коренско сертификационо тело (ERCA).

Контакт адреса ERCA је:

Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Centre (TP 580)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

ERCA преиспитује политике сертификација MSA, укључујући ову политику сертификације SRB-NA, ради усаглашености са захтевима утврђеним у политици сертификације ERCA. Циљ процеса преиспитивања је да се осигурају упоредиви нивои безбедности у свакој држави чланици. ERCA архивира извештаје о преиспитивању политике и политике сертификације NA у сврху упућивања.

ERCA пружа услуге сертификације кључева за MSCA који су повезани са датом MSA само ако исход преиспитивања политике сертификације MSA пружа довољно основа за процену да ће захтеви из политике сертификације ERCA бити испуњени. Наставак услуге сертификације кључева од стране ERCA за MSCA зависи од правовременог пријема извештаја о ревизији MSA (видети одељак 8.1) који доказују да MSCA и даље испуњава своје обавезе како је утврђено у одобреној политици сертификације MSA.

1.6.2 SRB-NA

Република Србија је именовала Министарство грађевинарства, саобраћаја и инфраструктуре (Закон о радном времену посаде возила у друмском превозу и тахографима, Службени гласник РС, бр. 96/15 и 95/18) за тело државе чланице SRB-NA.

Одговорности SRB-NA су следеће:

- Утврђивање и документовање политике сертификације NA у складу са свим важећим захтевима из политике сертификације ERCA и вођење рачуна о њеном одобрењу од стране ERCA. SRB-NA чини доступном за ERCA верзију политике сертификације SRB-NA на енглеском језику и води рачуна о верзији на српском језику.

- Одобравање CPS-а SRB-CA и потврђивање његове усаглашености са овом политиком. Ово се може постићи заједно са ревизијама усаглашености SRB-CA (видети поглавље 8).
- Обезбеђивање или организовање да политика SRB-NA буде доступна свим укљученим телима.
- Обезбеђивање да SRB-CA има ресурсе потребне за рад у складу са овом политиком сертификације.
- Одобрење безбедносних политика SRB-CA, SRB-CP и SRB-CIA.
- Захтевање да сви релевантни прописи које налажу Заједнички критеријуми за сертификацију безбедности уређаја буду испуњени током целог животног циклуса уређаја.

1.6.3 SRB-CA

SRB-CIA именује SRB-CA, које спроводи политику сертификације Републике Србије и пружа услуге сертификације и дистрибуције кључева персонализаторима компоненти SRB-CP у Србији.

SRB-CA документује своје спровођење политике сертификације SRB-NA у Општим правилима рада сертификационог тела (SRB-CA CPS). SRB-CA CPS је процедурални документ SRB-CA који детаљно описује како се свакодневно спроводи политика сертификације SRB-NA. Документ је сачинило SRB-CA и он је његово власништво. Он се третира као информација која подлеже ограничењима. SRB-CA садржај свог CPS-а чини доступним само на основу потребе за добијањем информација. SRB-CA CPS-ом се управља, он се преиспитује и мења на основу спроведених поступака контроле докумената.

Политика сертификације SRB-NA захтева да се процесом издавања тахографских картица обезбеди да датум ступања на снагу сертификата картице буде исти као датум почетка важења саме тахографске картице, како је кодирано у EF Identification.

Политика сертификације SRB-NA захтева да ERCA буде обавештено без одлагања о губитку, крађи или потенцијалној компромитацији сваког приватног кључа или симетричног главног кључа SRB-CA и да укаже на евентуалну накнадну истрагу и евентуалну меру NA.

SRB-CA ставља свој CPS на располагање SRB-NA. SRB-NA је одговорно да утврди да ли је SRB-CA CPS усаглашен са политиком сертификације SRB-NA. SRB-CA на захтев такође чини доступну верзију свог CPS-а ERCA.

SRB-CA по потреби води евиденцију о својим операцијама како би доказало усаглашеност са политиком сертификације SRB-NA и на захтев чини ту евиденцију доступном SRB-NA и/или ERCA. Притужбе од стране персонализатора компоненти SRB-CP у вези са услугама које пружа SRB-CA упућују се на адресу SRB-NA (за контакт адресу видети одељак 1.5.2).

1.7 Дефиниције и акроними

Акроним	Дефиниција
AES	Стандард напредног шифровања (енг. *Advanced Encryption Standard*)
CP	Политика сертификације (енг. *Certificate Policy*)
CPS	Општа правила рада сертификационог тела (енг. *Certification Practice Statement*)
SRB-CA	Сертификационо тело Републике Србије (енг. *Certification Authority of the Republic of Serbia*)
SRB-CIA	Тело за издавање картица Републике Србије (енг.*Card Issuing Authority of the Republic of Serbia*
SRB-CP	Персонализатор српских тахографских картица (енг. *Personalizer of Serbian Tachograph Cards*)
SRB-NA	Национално тело Републике Србије (*Serbian National Authority*)
SRB-NA-CP	Политика сертификације националног тела Републике Србије (енг. *Serbian National Authority Certificate Policy*)
DSRC	Систем наменске комуникације кратког домета (енг. *Dedicated Short Range Communications*)
CSR	Захтев за потпис сертификата (енг. *Certificate Signing Request*)
ЕК	Европска комисија
ECC	Криптографија елиптичних крива (енг. *Elliptic Curve Cryptography*)
EGF	Екстерни уређај GNSS-а (енг. *External GNSS Facility*)
EA	Европско тело (енг. *European Authority*)
ERCA	Европско коренско сертификационо тело (енг. *European Root Certification Authority*)
ERCA - CP	Европска политика издавања коренских сертификата и политика инфраструктуре симетричних кључева (енг. *European Root Certificate Policy and Symmetric Key Infrastructure Policy*)
ЕУ	Европска унија
GNSS	Глобални навигациони сателитски систем (енг. *Global Navigation Satellite System*)
HSM	Хардверски сигурносни модул (енг. *Hardware Security Module*)
ISMS	Систем управљања информационом безбедношћу (енг. *Information Security Management System*)

Акроним	Дефиниција
ISSO	Службеник за безбедност информационог система (енг. *Information System Security Officer*)
JRC	Заједнички истраживачки центар (енг. *Joint Research Centre*)
KDR	Захтев за дистрибуцију кључева (енг. *Key Distribution Request*)
KM	Главни кључ сензора кретања (енг. *Motion Sensor Master Key*)
K_{M-VU}	део VU у KM
K_{M-WC}	део WC у K_M
KID	Идентификациони кључ сензора кретања (енг. *Motion Sensor Identification Key*)
KP	Кључ за упаривање сензора кретања (енг. *Motion Sensor Pairing Key*)
K_{M-DSRC}	Главни кључ DSRC-а (енг. *DSRC Master Key*)
LKM	Означена порука о кључу (енг. *Labeled Key Message*)
MA	Узајамна аутентификација (енг. *Mutual Authentication*)
MoS	Сензор кретања (енг. *Motion Sensor*)
NA	Национално тело (енг. *National Authority*)
NCP	Стандардизована политика сертификације (енг. *Normalized Certificate Policy*)
PKI	Инфраструктура јавног кључа (енг. *Public Key Infrastructure*)
RFC	Захтев за коментар (енг. *Request for Comment*)
RSA	Ривест, Шамир и Адлеман (*Rivest, Shamir und Adleman*)
TC	Тахографска картица
VU	Јединица у возилу
WC	Картица радионице

Додатне дефиниције могу се наћи у документима на које упућује ова политика сертификације SRB-CA; видети одељак Упућивања на крају овог документа.

2 Одговорности у погледу објављивања и репозиторијума

2.1 Репозиторијуми

- Сви сертификати за уређај које издаје SRB-CA чувају се у бази података SRB-CA.

2.2 Објављивање информација о сертификацији

- SRB-NA објављује ову политику сертификације на свом веб сајту.
- Општа правила рада сертификационог тела SRB-CA нису јавна, али се на захтев достављају релевантним странама.

2.3 Време и учесталост објављивања

- Информације које се односе на промене ове политике објављују се према распореду дефинисаном у поступцима за промену (измену) утврђеним у одељку 9.12 овог документа.

2.4 Контроле приступа репозиторијумима

- За све информације које су доступне на веб сајту дозвољава се приступ само за читање. SRB-CA одређује особље које има приступ за писање или измену информација у SRB-CA CPS-у.
- Све информације објављене на веб сајту доступне су преко сигурне интернет везе.

3 Идентификација и аутентификација

Ово поглавље описује како се одвијају идентификација и аутентификација (ИиА) захтева за иницијално издавање сертификата и захтева за обнову сертификата са новим кључем, као и захтева за дистрибуцију симетричних кључева између SRB-CA и ERCA. ИиА између SRB-CA и произвођача уређаја или персонализатора картица детаљно су описане у SRB-CA CPS.

3.1 Додељивање имена

3.1.1 Врсте имена

3.1.1.1 Предмет сертификата и издавалац сертификата

Референтна ознака сертификационог тела и референтна ознака имаоца сертификата идентификују издаваоца и предмет сертификата. Оне се формирају на следећи начин, како је описано у Анексу IB, Додатак 11, CSM_136/CSM_141 и Додатак 1:

Субјект:

- SRB-CA

Идентификатор:

- Идентификатор кључа сертификационог тела (KID)

Структура:

- Нумерички код државе
- Алфанумерички код државе
- Серијски број кључа
- Додатне информације
- Идентификатор CA

Сертификати пробних кључева, захтеви за пробне сертификате, захтеви за дистрибуцију пробних кључева и поруке о дистрибуцији пробних кључева за потребе тестирања интероперабилности садрже вредности '54 4B' ("TK") у пољу *additionalInfo*.

3.1.1.2 Захтеви за дистрибуцију кључева и поруке о дистрибуцији кључева

Захтеве за дистрибуцију кључева и поруке за дистрибуцију кључева идентификује идентификатор кључева краткотрајног јавног кључа који генерише свако MSCA, видети одељак 4.2.1. Вредност идентификатора кључева одређује се у складу са одељком 3.1.1.1. са следећим изменама:

- keySerialNumber: јединствен за сваки субјект који подноси захтев
- additionallnfo: '4B 52' ("KR", за захтев за кључ), осим ако се не односи на пробни KDR. У том случају користи се '54 4B' ("TK", за пробни кључ).

3.2 Иницијално потврђивање идентитета

3.2.1 Начин за доказивање поседовања приватног кључа

Приликом подношења захтева за потписивање сертификата (CSR) ERCA, неопходан је доказ о поседовању одговарајућег приватног кључа интерним потписом, како је наведено у одељку 4.1.1. CSR-ови такође могу имати спољни потпис којим се доказује аутентичност поруке. Спољни потпис добија се помоћу већ сертификованог приватног кључа наведеног у CSR-у.

Провером (извршеном ручно заједно са MSA/MSCA), ако се хеш (распршивање) израчунат преко примљеног CSR-а подудара са хешом преко CSR-а који је послало MSCA (како је описано у CPS-у ERCA), добија се додатни доказ интегритета, аутентичности и почетног поверења.

3.2.2 Аутентификација идентитета организације

SRB-CA утврђује поступак за аутентификацију идентитета организација (нпр. произвођача уређаја) у свом CPS-у.

3.2.3 Аутентификација идентитета појединца

SRB-CA утврђује поступак за аутентификацију идентитета појединаца. Поступак је документован у CPS-у SRB-CA.

3.2.4 Валидација овлашћења

SRB-CA утврђује поступак за валидацију овлашћења у својим Општим правилима рада сертификационог тела.

3.2.5 Критеријуми за интероперабилност

SRB-CA се за услуге потписивања сертификата и дистрибуцију кључева које пружа систему паметних тахографа неће ослањати ни на једно спољно сертификационо тело већ само на ERCA.

Ако SRB-CA мора да се ослони на спољну PKI за неку другу услугу или функцију, пре подношења захтева за услуге сертификације потребно је да SRB-NA преиспита и одобри CP и/или CPS спољног пружаоца услуга сертификације.

3.3 Идентификација и аутентификација захтева за обнављање кључа (Re-Key)

Поступци идентификације и аутентификације захтева за обнову кључа (видети одељке 4.1.8. и 4.2.9) исти су као поступци описани у одељку 3.2.

3.4 Идентификација и аутентификација захтева за опозив

Захтеви за опозив сертификата које ERCA прими из било ког извора (видети одељак 4.1.10) потврђују се директном комуникацијом са MSA одговорном за MSCA имаоца сертификата, преко контакт тачке.

SRB-CA у свом CPS-у описује како ће потврдити захтеве за опозив сертификата за сертификате за уређај, ако су поступци за опозив сертификата расположиви.

4 Оперативни захтеви у погледу животног циклуса сертификата, симетричних кључева и услуга шифровања

Ово поглавље описује формате порука, криптографске механизме и поступке за захтеве за добијање и дистрибуцију сертификата за уређај, симетричних кључева за картице и услуге шифровања података о уређају и VU између SRB-CA и његових персонализатора компоненти SRB-CP, као и за захтев за издавање и дистрибуцију сертификата MSCA и симетричних главних кључева између ERCA и SRB-CA.

4.1 Захтев за добијање и издавање сертификата јавног кључа SRB-CA

4.1.1 Захтеви за потпис сертификата

Захтеве за потпис сертификата могу поднети само MSCA која је признало њихово MSA изјавом о усаглашености (видети 1.5.2).

CSR мора бити у формату TLV. Табела 1. приказује кодирање CSR-а, укључујући све тагове. За дужине се користе правила кодирања DER наведена у ISO/IEC 19790. Вредности су наведене у наставку овог одељка.

Објект података	**Req**	**Tag**
Аутентификација	c '67	
Сертификат ECC (CV)	m	'7F 21'
Тело сертификата	m	'7F 4E'
Идентификатор профила сертификата	m	'5F 29'
Референтна ознака сертификационог тела	m	'42'
Ауторизација имаоца сертификата	m	'5F 4C'
Јавни кључ	m	'7F 49'
Стандардизовани параметри домена OID	m	'06'
Јавна тачка	m	'86'
Референтна ознака имаоца сертификата	m	'5F 20'
Датум ступања на снагу сертификата	m	'5F 25'
Датум истека важења сертификата	m	'5F 24'
Унутрашњи потпис	m	'5F 37'
Референтна ознака сертификационог тела потписника спољног потписа	c	'42'
Спољни потпис	c	'5F 37'

Табела 1. Формат захтева за потписивање сертификата

m: захтева се
c: условно

Објект података **Аутентификација** присутан је само у случају да је присутан објекат података Спољни потпис.

Верзија профила идентификује се **идентификатором профила сертификата.** Верзија 1, наведена у одељку7.1, идентификује се вредношћу '00'.

Референтна ознака сертификационог тела користи се за информисање ERCA о приватном кључу ERCA који SRB-CA очекује да буде коришћен за потписивање сертификата. За вредности референтне ознаке сертификационог тела видети одељак 3.1_. У сваком датом тренутку, идентификатор кључа коренског кључа ERCA који је доступан за потписивање биће назначен на веб сајту ERCA.

Ауторизација имаоца сертификата користи се за идентификовање врсте сертификата. Састоји се од шест најзначајнијих бајтова идентификационе ознаке апликације тахографа ('FF 53 4D 52 44 54'), уланчених са врстом уређаја коме је сертификат намењен (Анекс IB, Додатак 11, CSM141). За сертификате MSCA, тип уређаја се поставља на '0E' (14 децимала).

Јавни кључ садржи два објекта података:

- Објект података **Параметар домена** упућује на стандардизоване параметре домена који ће се користити са јавним кључем у сертификату. Он садржи један од идентификатора објекта наведених у табели 1. Додатка 11, Анекс IB.
- Објект података **Јавна тачка** мора садржати јавну тачку. Јавне тачке елиптичне криве претварају се у октетни низ како је наведено у ISO/IEC 18033-2. Користи се декомпримовани формат кодирања (Анекс IB, Додатак 11, CSM_143).

Референтна ознака имаоца сертификата користи се за идентификацију јавног кључа садржаног у захтеву и у креираном сертификату. Референтна ознака имаоца сертификата мора бити јединствена. Она се може користити за упућивање на овај јавни кључ у сертификатима на нивоу уређаја (Анекс IB, Додатак 11, CSM_144). За вредности референтне ознаке имаоца сертификата видети одељак 3.1_.

Датум ступања на снагу сертификата садржи датум почетка важења и период важења сертификата. **Датум истека важења сертификата** садржи датум престанка важења и период важења сертификата. Оба елемента података морају бити врсте података TimeReal, наведене у Анексу IB, Додатак 11. Напомиње се да је период важења дефинисан са ова два елемента података или 17 година и 3 месеца (за сертификате MSCAVU-EGF) или 7 година и 1 месец (за сертификате MSCACard).

Тело сертификата је самопотписано **унутрашњим потписом** који се може проверити јавним кључем садржаним у захтеву за издавање сертификата. Потпис се креира преко кодираног тела сертификата, укључујући таг и дужину тела сертификата. Алгоритам потписа је ECDSA, како је наведено у ISO/IEC 10116, уз коришћење алгоритма хеширања повезаног са величином јавног кључа у CSR-у, како је наведено у Анексу IB, Додатак 11, CSM_50. Формат потписа мора бити обичан, како је наведено у ISO/IEC 18033-2.

Референтна ознака сертификационог тела потписника спољног потписа садржи MSCA и одговарајући кључ који је ставио спољни потпис. Она је присутна само ако је присутан спољни потпис. За могуће вредности видети одељак 3J_.

Спољни потпис није присутан ако SRB-CA поднесе захтев за свој иницијални сертификат. Спољни потпис потребан је ако SRB-CA поднесе захтев за сукцесивни сертификат. У том случају, Захтев за потпис сертификата додатно потписује SRB-CA спољним потписом, користећи један од тренутно важећих приватних кључева SRB-CA. Спољни потпис потврђује веродостојност захтева. Пошто је SRB-CA претплаћено

на добијање и MSCA_Card и MSCA_VU-EGF сертификата, спољни потпис ставља се коришћењем приватног кључа повезаног са сертификатом исте врсте.

Спољни потпис креира се преко кодираном сертификату ECC (CV) (укључујући таг '7F 21' сертификата и његову дужину) и поља Референтна ознака сертификационог тела потписника спољног потписа (укључујући таг '42' сертификата и његову дужину). Алгоритам потписа је ECDSA, како је наведено у ISO/IEC 10116, уз коришћење алгоритма хеширања повезаног са величином кључа SRB-CA који се користи за потпис, како је наведено у Анексу IB, Додатак 11, CSM_50. Формат потписа мора бити обичан, како је наведено у ISO/IEC 18033-2.

SRB-CA израчунава и складишти хеш преко комплетног CSR-а, користећи алгоритам хеширања повезан са величином кључа овлашћења за потписивање, како је наведено у Анексу IB, Додатак 11, CSM_50. Овај хеш користиће ERCA заједно са MSA/MSCA за ручну проверу аутентичности CSR-а, видети одељак 4.1.2.1.

4.1.2 Обрада захтева за сертификат

4.1.2.1 Провера садржаја CSR-а

ERCA обезбеђује да је CSR који долази од било ког MSCA потпун, тачан и прописно ауторизован. ERCA потписује MSCA сертификат само у том случају.

Провере исправности, потпуности и ауторизације врше службеници ERCA ручно и/или их аутоматизовано врши служба за регистрацију ERCA. Ако је захтев исправан и потпун, службеници ERCA одобравају потписивање сертификата MSCA.

За сваки CSR који добије, ERCA провера следеће:

- да ли је медијум за пренос података читљив, тј. да није оштећен или неисправан;
- да ли је формат CSR-а у складу са Табелом 2;
- да ли је захтев прописно ауторизован. Ако постоји спољни потпис, ERCA проверава исправност тог потписа. У сваком случају, ERCA контактира MSCA како је описано у ERCA CPS и проверава да ли се хеш израчунат преко примљеног CSR-а поклапа са хешом преко CSR-а који је послао MSCA;
- да ли MSCA има право да добије тражену врсту сертификата;
- да ли референтна ознака сертификационог тела садржана у захтеву садржи коренски приватни кључ ERCA који је тренутно важећи за потписивање сертификата MSCA;
- да ли је референтна ознака имаоца сертификата јединствена. За MSCA, референтна ознака имаоца сертификата је идентификатор кључа сертификационог тела (KID). Серијски број кључа у овом KID-у разликује се од кључева истог MSCA, због чега је KID јединствен;
- да ли су параметри домена прецизирани у захтеву наведени у Табели 1. Анекса IB, Додатак 11, а јачина ових параметара се поклапа са јачином коренског кључа ERCA наведеног у референтној ознаци сертификационог тела;
- да јавна тачка у захтеву није претходно сертификована од стране ERCA и да није раније коришћена као краткотрајни кључ за дистрибуцију симетричног кључа (видети одељак 4.2.3), чак ни у сврхе испитивања интероперабилности;
- да ли се јавна тачка из захтева налази на кривој назначеној у захтеву;
- да се унутрашњи потпис може проверити коришћењем јавне тачке и параметара домена наведених у захтеву. Ово доказује да MSCA поседује приватни кључ повезан са јавним кључем;

- да је спољни потпис присутан ако захтев није поднет за иницијални сертификат MSCAVU-EGF или MSCACard MSCA;
- да се, ако постоји, спољни потпис може проверити коришћењем јавне тачке и параметара домена у сертификату MSCA на које се упућује у пољу Референтна ознака сертификационог тела потписника спољног потписа. Поред тога, да период коришћења приватног кључа овог кључа још увек није истекао.

Ако било која од ових провера не успе, ЕРЦА одбија CSR. ERCA доставља образложење за сваки одбијени захтев MSCA и надлежном MSA.

4.1.2.2 Генерисање, дистрибуција и управљање сертификатима

Ако су све провере успешне, ERCA наставља са потписивањем сертификата како је описано у одељку 4.1.3.

Следеће информације бележе се у бази података ERCA за сваки примљени захтев за потпис сертификата:

- комплетан CSR који потиче од MSCA;
- комплетан креирани сертификат јавног кључа, ако постоји;
- стандардизовани параметри домена OID и јавна тачка сертификованог јавног кључа;
- ефективни подаци о сертификату и датум истека важења сертификата;
- референтна ознака имаоца сертификата (за идентификацију јавног кључа);
- хеш преко бинарних података сертификата, ако постоје. Дужина хеша повезана је са величином кључа овлашћења за потписивање, како је наведено у Анексу IB, Додатак 11, CSM_50;
- хеш преко бинарних података CSR-а, видети одељак 4.1.1;
- статус сертификата „Важећи” ако је сертификат издат или статус „Одбијен” у случају да је CSR одбијен;
- временски жиг.

Сертификати MSCA уписују се на медијуме за пренос података у складу са захтевима из одељка 4.1.4, за враћање у MSCA. Свака копија сертификата уписана на медијуму за пренос података накнадно се проверава помоћу јавног кључа ERCA. ERCA такође уписује на медијум за пренос података копију сертификата јавног кључа ERCA која се може користити за проверу сертификата MSCA.

Након успешне дистрибуције новог сертификата MSCA, ERCA ажурира информације о статусу сертификата у репозиторијуму ERCA. Не спроводи се ниједна друга активност обавештавања. ERCA задржава медијуме за пренос података са CSR-ом и архивира их у својим контролисаним просторијама. ERCA настоји да заврши операције сертификације јавних кључева у року од једног радног дана. Време потребно да ERCA достави MSCA сертификат јавног кључа или дистрибуира симетрични кључ одређено је искључиво временом потребним за исправно спровођење процедура ERCA. Гарантује се време обраде од једног месеца. Када се подноси захтев за сертификат, MSCA узимају у обзир то максимално време обраде.

4.1.3 Сертификати

Формат сертификата јавног кључа MSCA може се наћи у одељку 7_1.

ERCA креира потпис преко кодираног тела сертификата, укључујући таг и дужину тела сертификата. Алгоритам потписа је ECDSA, како је наведено у ISO/IEC 10116, уз коришћење алгоритма хеширања повезаног са величином кључа овлашћења за потписивање, како је наведено у Анексу IB, Додатак 11, CSM_50. Формат потписа мора бити обичан, како је наведено у ISO/IEC 18033-2.

4.1.4 Размена захтева и одговора

За пренос захтева за потписивање сертификата и сертификата треба користити CD-R медијуме:

- CD-R треба да буде медијум од 12 cm у режиму једне сесије (форматиран према ISO 9660:1988).

Друге методе преноса могу се користити уз претходну сагласност ERCA. У сврху тестирања, ERCA прихвата и шаље CSR-ове и сертификате као прилоге уз електронску пошту.

SRB-CA уписује на медијум за пренос података три копије сваког захтева за потписивање сертификата за пренос до ERCA. Ове копије су у хексадецималном ASCII формату (датотека .txt), Base64 формату (датотека .pem) и бинарном формату (датотека .bin).

ERCA уписује на медијум за пренос података три копије сваког сертификата за враћање SRB-CA. Ове копије су у хексадецималном ASCII формату (датотека .txt), Base64 формату (датотека .pem) и бинарном формату (датотека .bin).

Уз сваки захтев за потпис сертификата и сертификат прилаже се штампани примерак података, форматиран према шаблону утврђеном у CPS-у ERCA. Један штампани примерак података чува ERCA, односно SRB-CA.

И у случају CSR-а и сертификата, медијуме за пренос података и штампане материјале размењују службеник ERCA и курир SRB-CA у контролисаном подручју ERCA.

4.1.5 Прихватање сертификата

Курир потписује пријем сертификата SRB-CA у просторијама ERCA. По пријему сертификата у просторијама SRB-CA, SRB-CA проверава следеће:

- да ли је медијум за пренос података читљив, тј. да није оштећен или неисправан;
- да ли је формат сертификата је у складу са Табелом 9. у одељку 7.1;
- да ли све вредности поља у сертификату одговарају вредностима захтеваним у CSR-у;
- да ли се потпис сертификата може проверити коришћењем коренског јавног кључа ERCA наведеног у пољу CAR.

Ако нека од ових провера не успе, SRB-CA прекида поступак и контактира ERCA. Сертификат се одбија према поступку за опозив сертификата (видети одељак 4.1.10).

4.1.6 Коришћење пара кључева и сертификата

SRB-CA користи сваки пар кључева и одговарајући сертификат у складу са одељком 6.2.

4.1.7 Обнављање сертификата

Обнављање сертификата, тј. продужење рока важења постојећег сертификата није дозвољено.

4.1.8 Обнова сертификата са новим кључем

Обнова сертификата са новим кључем значи потписивање новог сертификата SRB-CA који замењује постојећи сертификат. Обнова сертификата са новим кључем врши се у следећим случајевима:

- када се SRB-CA ближи крају периода коришћења (једног од) својих приватних кључева. У овом случају обнова сертификата са новим кључем врши се правовремено како би се обезбедило да SRB-CA може да настави са радом по истеку овог периода;
- након опозива сертификата.

Захтев за сертификат, обрада, издавање, прихватање и објављивање сертификата исти су као и за првобитни пар кључева. SRB-CA одмах дистрибуира неопходне кључеве и сертификате персонализаторима компоненти SRB-CP како је даље описано у SRB-CA CPS.

Парови кључева MSCA могу се редовно мењати. ERCA не може наметати никаква ограничења у погледу броја сертификата MSCA које ће потписати. MSCA је дозвољено да затражи више сертификата MSCA исте врсте чији се периоди важења преклапају ако је то оправдано за њихову делатност.

4.1.9 Измена сертификата

Измена сертификата није дозвољена.

4.1.10 Опозив и суспензија сертификата

4.1.10.1 Околности за опозив сертификата

Сертификати SRB-CA опозивају се у следећим околностима:

- одбијање по пријему новоиздатог сертификата (видети одељак 4.1.5);
- приватни кључ SRB-CA је компромитован или се сумња да је компромитован;
- губитак приватног кључа SRB-CA;
- укидање SRB-CA;
- неиспуњавање обавеза у складу са Уредбом и политиком сертификата ERCA од стране SRB-NA или SRB-CA.

4.1.10.2 Ко може захтевати опозив

ERCA сматра меродавним захтеве за опозив који потичу од следећих субјеката:

- Европско тело;
- сва NA;
- сва призната MSCA;

Европско тело овлашћено је да захтева опозив свих сертификата MSCA. MSA овлашћено је да захтева опозив сертификата издатих за MSCA која су наведена у политици сертификације MSA.

MSCA је овлашћено да захтева опозив сертификата који су издати самом MSCA. ERCA одбија захтеве за опозив који потичу од било ког другог субјекта.

4.1.10.3 Поступак у случају захтева за опозив

Поступак опозива сертификата документован је у SRB-CA CPS.

4.1.10.4 Период одлагања захтева за опозив

Дозвољен период одлагања захтева за опозив сертификата је пет радних дана од наступања околности за опозив и у том року претплатник мора поднети захтев за опозив.

4.1.10.5 Рок у ком ERCA обрађује захтев за опозив

ERCA обрађује исправне, потпуне и одобрене захтеве за опозив у року од три радна дана од пријема.

4.1.10.6 Захтеви за проверу опозива за трећа лица

Трећа лица одговорна су за проверу информација о статусу сертификата објављених у репозиторијуму ERCA.

4.1.10.7 Учесталост издавања статуса сертификата

Статус сертификата јавних кључева ERCA и MSCA може се преузети онлајн са https://dtc.irc.ec.europa.eu/. ERCA одржава интегритет информација о статусу опозива сертификата.

Информације о статусу сертификата објављене у репозиторијуму ERCA ажурирају се првог радног дана сваке недеље.

4.1.10.8 Максимално време чекања за CRL

Није примењиво.

4.1.10.9 Доступност онлајн провере опозива/статуса

Доступност информација о опозиву/статусу објављених у репозиторијуму ERCA гарантује се само за време редовног радног времена.

4.1.10.10 Захтеви за онлајн проверу опозива/статуса

Нема захтева.

4.1.10.11 Други доступни облици оглашавања опозива

Нема их.

4.1.10.12 Посебни захтеви у вези са компромитацијом кључа

Компромитација приватног кључа је безбедносни инцидент који треба обрадити.

Ако је један од приватних кључева SRB-CA компромитован или постоји сумња да је компромитован, SRB-CA пријављује инцидент ERCA и SRB-NA без непотребног одлагања, бар у року од 8 сати од откривања. SRB-CA у свом обавештењу наводи околности под којима је дошло до компромитације.

Предузимају се истрага и могуће мере од стране SRB-NA и/или SRB-CA да би се смањио ризик од злоупотребе компромитованог кључа.

ERCA се обавештава о исходу истраге SRB-NA.

4.1.11 Суспензија сертификата

Суспензија сертификата није дозвољена.

4.1.12 Услуга провере статуса сертификата

Доступност веб сајта поменутог у одељку 4.1.10.7. гарантује се за време редовног радног времена. Списак информација о статусу сертификата MSCA се такође може преузети са овог веб сајта у општеприхваћеном формату датотеке (нпр. .csv, Excel).

4.1.13 Крај претплате

Коришћење услуга потписивања сертификата ERCA престаје када SRB-NA одлучи о престанку рада SRB-CA. SRB-NA обавештава ERCA о тој промени која представља промену политике сертификације SRB-NA.

У случају престанка претплате, SRB-NA одлучује о томе да ли се подноси захтев за опозив сертификата за све важеће сертификате SRB-CA или се дозвољава да сви сертификати SRB-CA истекну.

4.1.14 Депоновање (escrow) и опоравак кључа

Депоновање кључева је изричито забрањено, што значи да коренски приватни кључеви SRB-CA никада неће бити извезени или похрањени у другом систему осим у производном и резервном систему SRB-CA.

4.2 Захтев за симетрични главни кључ и његова дистрибуција између ERCA и SRB-CA

Следећи захтеви у великој мери се заснивају на одговарајућем поглављу политике сертификације ERCA друге генерације.

4.2.1 Захтеви за дистрибуцију кључева

Захтеве за дистрибуцију кључева могу поднети само MSCA које је признало њихово MSA изјавом о усаглашености (видети 1.5.2).

KDR мора бити у формату TLV. Табела 2. приказује кодирање KDR-а, укључујући све тагове. За дужину се користе правила кодирања DER наведена у ISO/IEC 19790. Вредности су наведене у наставку овог одељка.

Објект података	**Req**	**Таг**
Захтев за дистрибуцију кључева	m	'A1'
Идентификатор профила захтева	m	'5F 29'
Ауторизација примаоца поруке	m	'83'
Идентификатор кључа	m	'84'
Јавни кључ (за ECDH протокол за усаглашавање кључева)	m	'7F 49'
Стандардизовани параметри домена OID	m	'06'
Јавна тачка	m	'86'

Табела 2. Формат захтева за дистрибуцију кључа

Верзија профила идентификује се **идентификатором профила захтева.** Верзија 1, наведена у Табели 2. идентификује се вредношћу ‘00’.

Ауторизација примаоца поруке користи се за идентификацију симетричног кључа који се захтева. Састоји се од уланчавања

- шест најзначајнијих бајтова идентификационе ознаке апликације тахографа ('FF 53 4D 52 44 54'),
- врсте кључа који се захтева (видети у наставку, 1 бајт),
- броја верзије захтеваног главног кључа (1 бајт).

Следеће вредности користе се за означавање врсте кључа који се захтева:

- '07' K_M, главни кључ сензора кретања
- '27': K_M, радионички део главног кључа сензора кретања
- '67': $K_{M\text{-}VU}$, део VU главног кључа сензора кретања
- '09': $K_{M\text{-}DSRC}$, главни кључ DSRC-а

Идентификатор кључа је јединствени низ октета од 8 битова који идентификује јавни кључ приказан у KDR-у за размену кључева ECDH-а, видети одељак 4.2.3. Његова вредност одређена је у складу са одељком 3.1.1.2. Пошто MSCA користи другачији пар краткотрајних кључева за сваки захтев за дистрибуцију кључа, SRB-CA може користити идентификатор кључа да прати краткотрајни приватни кључ који ће се користити за дешифровање одређене поруке о дистрибуцији кључева када та порука стигне до SRB-CA. Из тог разлога ERCA копира идентификатор кључа у поруци о дистрибуцији кључа, видети Табелу 3.

Јавни кључ садржи два елемента податка:

- Елемент податка Public Point садржи јавну тачку краткотрајног пара кључева SRB-CA који ће се користити за усаглашавање кључева. SRB-CA конвертује јавну тачку у октетни низ како је наведено у ISO/IEC 18033-2, користећи декомпримовани формат кодирања.
- Елемент податка Domain Parameters садржи идентификатор објекта скупа стандардизованих параметара домена који ће се користити заједно са јавном тачком. За више информација видети одељак 4.2.3.

SRB-CA израчунава и складишти хеш преко комплетног KDR-а, користећи алгоритам хеширања повезан са величином кључа захтеваног главног кључа, како је наведено у Анексу IB, Додатак 11, CSM_50. Овај хеш користиће ERCA за проверу аутентичности KDR-а, видети одељак 4.2.2.1.

4.2.2 Обрада захтева за главни кључ

4.2.2.1 Провера садржаја KDR-а

ERCA обезбеђује да је KDR који долази од SRB-CA потпун, тачан и прописно ауторизован. ERCA само у том случају креира поруку о дистрибуцији кључа.

Провере исправности, потпуности и ауторизације врше службеници ERCA ручно и/или их аутоматизовано врши служба за регистрацију ERCA. Ако је захтев исправан и потпун, службеници ERCA могу ауторизовати генерисање поруке о дистрибуцији кључева које врши служба за дистрибуцију кључева. За сваки KDR који добије, ERCA провера следеће:

- да ли је медијум за пренос података читљив, тј. да није оштећен или неисправан;

- да ли је формат KDR-а у складу са Табелом 2;
- да ли је захтев прописно ауторизован. ERCA контактира SRB-CA како је описано у CPS-у ERCA и проверава да ли се хеш израчунат преко примљеног KDR-а поклапа са хешом преко KDR-а који је ускладиштио SRB-CA (видети крај одељка 4.2.1);
- да ли SRB-CA има право да добије тражену врсту главних кључева;
    - SRB-CA који су одговорни за издавање тахографских картица имају право да добију све важеће верзије $K_{M\text{-}WC}$ у вези са коришћеним пакетом шифри и мастер кључем DSRC-а $K_{M\text{-}DSRC}$;

4.2.2.2 Генерисање, дистрибуција и администрација KDM-а

Ако су све провере успешне, ERCA наставља са припремањем поруке о дистрибуцији кључа одређивањем симетричног кључа који је захтевао SRB-CA, следећи кораке описане у одељку 4.2.3 (од корака 2). Следеће информације бележе се у бази података ERCA за сваки примљени захтев за дистрибуцију кључа:

- комплетан KDR који потиче од SRB-CA;
- комплетна креирана порука о дистрибуцији кључа, ако постоји;
- стандардизовани параметри домена OID, краткотрајна јавна тачка и идентификатор кључа;
- врста кључа и верзија главног кључа;
- хеш преко бинарних података поруке о дистрибуцији кључа, ако постоји. Дужина хеша повезана је са величином кључа овлашћења за потписивање, како је наведено у Анексу IB, Додатак 11, CSM_50;
- хеш преко бинарних података KDR-а, видети одељак 4.2.1;
- статус „Distributed (дистрибуиран)" у случају да се кључ дистрибуира SRB-CA или „Rejected (одбијен)" у случају да је KDR одбијен;
- временски жиг.

ERCA задржава медијуме за пренос података са KDR-ом и архивира их у својим контролисаним просторијама.

Када се генерише порука о дистрибуцији кључа, ERCA је шаље MSCA, како је наведено у одељку 4.2.5.

ERCA настоји да заврши операције дистрибуције кључева у року од једног радног дана. Гарантује се време обраде од једног месеца. Приликом подношења захтева за дистрибуцију кључа, SRB-CA узимају у обзир то максимално време обраде.

4.2.3 Заштита поверљивости и аутентичности симетричних кључева

Поверљивост и аутентичност симетричних кључева које ERCA дистрибуира до SRB-CA заштићене су шемом интегрисаног шифровања применом елиптичних крива (ECIES). Ова шема омогућава усаглашавање између ERCA и SRB-CA о кључевима за шифровање и кључевима MAC који ће се користити за заштиту главних симетричних кључева током дистрибуције. ECIES је стандардизован у ISO/IEC 18033-2. Варијанта ECIES-а која ће се користити за дистрибуције симетричних кључева ERCA користи следеће криптографске алгоритме, у складу са Додатком 11. Анекса IB:

- Функција извођења кључа: KDF2, како је наведено у ISO/IEC 18033-2;

- Кодни алгоритам за аутентификацију поруке: Алгоритам AES у режиму CMAC, како је наведено у NIST, Посебна публикација 800-38B;
- Алгоритам симетричне енкрипције: AES у режиму рада „уланчавање шифрираних блокова" - (*Cipher Block Chaining* - CBC), како је утврђено у ISO/IEC 10116.

На вишем нивоу ECIES се састоји од следећих корака. Више појединости за сваки корак дато је у наставку:

1. MSCA генерише јединствени краткотрајни пар кључева ECC за Дифи-Хелманово усаглашавање кључева и шаље јавни кључ ERCA у Захтеву за дистрибуцију кључева, видети Табелу 2.
2. ERCA на сличан начин генерише јединствени краткотрајни ECDH пар кључева и користи Дифи-Хелманов алгоритам за усаглашавање кључева заједно са сопственим приватним кључем и краткотрајним јавним кључем MSCA за извођење дељене тајне.
3. Користећи функцију извођења кључа, дељену тајну и додатне информације прецизније наведене у наставку, ERCA изводи кључ за шифровање и кључ MAC-а.
4. ERCA користи кључ за шифровање да би шифровало симетрични кључ који треба дистрибуирати.
5. ERCA користи кључ MAC-а да израчуна MAC преко шифрованог кључа.

<u>Корак 1</u>

За генерисање свог краткотрајног јавног кључа који се користи за Дифи-Хелманово усаглашавање кључева, SRB-CA бира један од стандардизованих параметара домена из Табеле 1. Анекса IB, Додатак 11. Јачина изабраног скупа параметара домена одговара дужини захтеваног симетричног кључа, према CSM_50 у Додатку 11. Генерисање краткотрајног пара кључева одвија се у HSM-у који испуњава захтеве из одељка 6.2. Краткотрајни приватни кључ никада не напушта HSM.

Након генерисања краткотрајног пара кључева, SRB-CA конвертује јавну тачку у октетни низ, како је прецизирано у ISO/IEC 18033-2. Користи се декомпримовани формат кодирања. SRB-CA укључује OID изабраних стандардизованих параметара домена и октетни низ који представља јавну тачку у KDR-у, који се шаље ERCA.

<u>Корак 2</u>

ERCA генерише краткотрајни пар кључева, користећи стандардизоване параметре домена наведене у примљеном KDR-у. ERCA користи алгоритам ECKA-DH како је утврђено у ISO/IEC 18033-2 заједно са сопственим краткотрајним приватним кључем и краткотрајним јавним кључем SRB-CA за извођење дељене тачке (K_x, K_y). ERCA проверава да ова тачка није тачка у бесконачности. Ако јесте, ERCA генерише нови пар краткотрајних кључева и покушава поново. У супротном, ERCA формира дељену тајну K тако што ће конвертовати Kx у октетни низ како је наведено у ISO/IEC 18033-2.

Генерисање краткотрајног пара кључева одвија се у HSM-у који испуњава захтеве из одељка 6.2. Краткотрајни приватни кључ никада не напушта HSM.

<u>Корак 3</u>

За извођење кључа за шифровање K_{ENC} и кључа за MAC- ing K_{MAC}, , ERCA користи функцију извођења кључа KDF2(x, l) утврђену у ISO/IEC 18033-2. Октетни низ x једнак је дељеној тајни K из претходног корака. Хеш функција која је неопходна за

инстанцирање функције KDF2 повезана је са дужином симетричног кључа који се дистрибуира, како је описано у Додатку 11. CSM_50. Излазна дужина l једнака је излазној дужини ове хеш функције.

С обзиром на излаз O ове функције извођења кључа, кључеви за шифровање и MAC-ing формирају се као

- K_{ENC} = први L октети из O
- K_{MAC} = последњи L октети из O

где је L захтевана дужина K_{ENC} и K_{MAC} у октетима, у складу са Додатком 11. CSM_50.

Корак 4

Ако је потребно (тј. за 192-бајтни кључ), ERCA попуњава симетрични кључ који се дистрибуира коришћењем метода попуњавања (*padding*) 2. утврђеног у ISO/IEC 9797-1. Након тога, ERCA шифрује попуњени кључ помоћу AES-а у режиму рада „уланчавање шифрираних блокова" (CBC), како је утврђено у ISO/IEC 10116, користећи K_{ENC} са параметром преплитања (*interleave*) m = 1 и вектором иницијализације SV који се састоји од бинарних нула:

Шифровани симетрични кључ = AES-CBC (симетрични кључ + попуњавање по потреби, K_{ENC})

Корак 5

ERCA уланчава шифровани симетрични кључ са низом S, који је уланчавање вредности ауторизације примаоца поруке и идентификатора кључа који се користи у поруци о дистрибуцији кључа (видети одељак 4.2.4)

S = Ауторизација примаоца поруке || Идентификатор кључа

Користећи K_{MAC}, ERCA затим израчунава MAC преко уланчавања шифрованог симетричног кључа и S, користећи алгоритам AES у режиму CMAC, како је наведено у NIST, Посебна публикација 800-38B. Дужина MAC повезана је са дужином сесијских кључева AES, како је наведено у Додатку 11, CSM_50.

MAC = AES-CMAC (шифровани симетрични кључ || S, K_{MAC})

Све операције са краткотрајним приватним кључем, са дељеном тајном и са изведеним кључевима K_{ENC} и K_{MAC} одвијају се у HSM-у који испуњава захтеве из одељка 6.2.

ERCA бележи вредност S и MAC-а. Како је описано у одељку 4.2.6, SRB-CA ће ове вредности користити за проверу аутентичности поруке о дистрибуцији кључа.

4.2.4 Поруке о дистрибуцији кључева

Након обраде захтева за главни кључ (видети одељак 4.2.2), ERCA саставља поруку о дистрибуцији кључа како је приказано у Табели 3. За дужине се користе правила кодирања DER наведена у ISO/IEC 8825-1. Вредности су наведене у наставку овог одељка.

Објект података	**Req**	**Таг**
Дистрибуција кључева	m	'A1'
Идентификатор профила захтева	m	'5F 29'
Ауторизација примаоца поруке	m	'83'
Идентификатор кључа краткотрајног пара кључева MSCA за ECDH усаглашавање кључева	m	'84'
Јавна тачка ERCA за усаглашавање кључева ECDH	m	'86'
Шифровани симетрични кључ	m	'87'
MAC	m	'88'

Табела 3. Формат поруке о дистрибуцији кључа

Верзија профила идентификује се **идентификатором профила захтева**. Верзија 1, наведена у Табели 3. идентификује се вредношћу '00'.

Ауторизација примаоца поруке идентична је елементу податка ауторизације примаоца поруке у KDR-у од SRB-CA, видети одељак 4.2.1.

Јавна тачка садржи јавну тачку краткотрајног пара кључева ERCA који се користи за усаглашавање кључева, видети одељак 4.2.3. ERCA конвертује јавну тачку у октетни низ како је наведено у Техничким смерницама TR-03111 BSI, користећи декомпримовани формат кодирања.

Елемент податка **шифрованог симетричног кључа** садржи излаз из корака 4. у одељку 4.2.3.

Елемент податка MAC садржи излаз из корака 5. у одељку 4.2.3.

Након успешног генерисања поруке о дистрибуцији кључа, ERCA безбедно уништава свој краткотрајни приватни кључ за усаглашавање кључева у HSM-у, као и кључ за шифровање KENC и кључ за MAC- ing K_{MAC}. Порука о дистрибуцији кључа се враћа MSCA који је издао KDR.

4.2.5 Размена захтева и одговора

За пренос захтева за дистрибуцију кључева и порука о дистрибуцији кључева треба користити CD-R:

- - CD-R треба да буде медијум од 12 cm у режиму једне сесије (форматиран према ISO 9660:1988).

Друге методе преноса могу се користити уз претходну сагласност ERCA. У сврху тестирања, ERCA прихвата и шаље захтеве за дистрибуцију кључева и поруке о дистрибуцији кључева као прилоге уз електронску пошту.

SRB-CA уписује на медијум за пренос података три копије сваког захтева за дистрибуцију кључева за пренос до ERCA. Ове копије су у хексадецималном ASCII формату (датотека .txt), Base64 формату (датотека .pem) и бинарном формату (датотека .bin).

ERCA уписује на медијум за пренос података три копије сваке поруке о дистрибуцији кључева за враћање SRB-CA. Ове копије су у хексадецималном ASCII формату (датотека .txt), Base64 формату (датотека .pem) и бинарном формату (датотека .bin).

Уз сваки KDR и KDM прилаже се штампани примерак података, форматиран према шаблону утврђеном у CPS-у ERCA. Један штампани примерак података чува ERCA, односно SRB-CA.

Иу случају KDR и KDM, медијуме за пренос података и штампане материјале размењују службеник ERCA и курир SRB-CA у контролисаном подручју JRC-а.

4.2.6 Прихватање главног кључа

Курир потписује пријем поруке о дистрибуцији кључева у просторијама ERCA. По пријему поруке о дистрибуцији кључева у просторијама MSCA, SRB-CA проверава следеће:

- да ли је медијум за пренос података читљив, тј. да није оштећен или неисправан;
- да ли је формат поруке у складу са Табелом 3;
- да ли је порука оригинална. SRB-CA то чини тако што контактира ERCA како је описано у CPS-у ERCA и проверава да ли се MAC у примљеној KDM поклапа са MAC-ом у KDM коју је послао ERCA;
- врста и верзија главног кључа у поруци одговарају захтеваној врсти и верзији;
- јавна тачка наведена у поруци налази се на кривој одређеној захтевом за дистрибуцију кључа који SRB-CA шаље ERCA.

Ако нека од ових провера не успе, SRB-CA прекида поступак и контактира ERCA. Ако су све ове провере успешне, SRB-CA

- користи алгоритам ECKA-DH за извођење дељене тачке (Kx, Ky), како је описано у кораку 3. у одељку 4.2.3, користећи краткотрајни приватни кључ SRB-CA назначен идентификатором кључа у поруци и краткотрајним јавним кључем ERCA. MSCA проверава да дељена тачка није тачка у бесконачности; ако јесте, SRB-CA прекида процес и контактира ERCA. У супротном, SRB-CA формира дељену тајну K тако што ће конвертовати Kx у октетни низ како је наведено Техничким смерницама TR-03111 BSI;
- изводи кључеве KENC и KMAC како је описано у кораку 4. у одељку 4.2.3;
- проверава MAC преко шифрованог симетричног кључа, како је описано у кораку 5. у одељку 4.2.3. Ако нека од ових провера не успе, MSCA прекида поступак и контактира ERCA.
- дешифрује симетрични кључ, како је описано у кораку 4. у одељку 4.2.3. SRB-CA проверава да ли је попуњавање дешифрованог кључа, ако оно постоји, исправно. Ако нека од ових провера не успе, SRB-CA прекида поступак и контактира ERCA.

Све операције са краткотрајним приватним кључем, са дељеном тајном и са изведеним кључевима KENC и K_{MAC} одвијају се у HSM-у који испуњава захтеве из одељка 6.2.

Након успешног опоравка главног кључа или ако је процес дистрибуције кључева прекинут и није покренуто обнављање KDM-а (видети одељак 4.2.8), SRB-CA безбедно уништава свој краткотрајни приватни кључ за усаглашавање кључева у HSM-у, као и кључ за шифровање K_{ENC} и кључ за MAC- ing K_{MAC}.

4.2.7 Коришћење главног кључа

SRB-CA користи сваки примљени главни кључ у складу са одељком 6.2.

4.2.8 Обнављање KDM

Обнављање KDM значи издавање копије постојеће KDM за SRB-CA без промене краткотрајног јавног кључа или других информација у KDM-у.

Обнављање KDM може се извршити само ако је оригинални медијум за пренос података стигао у MSCA оштећен или неисправан. Оштећење или неисправност медијума за пренос података је безбедносни инцидент који се пријављује SRB-NA и ERCA. Након тог извештаја, SRB-CA може послати ERCA захтев за обнављање KDM-а, позивајући се на оригинални захтев за дистрибуцију кључева. Овај поступак је описан у CPS-у ERCA. ERCA прихвата само захтев за обнављање KDM оверен од стране SRB-NA које је одобрило SRB-CA. Напомена: У случају да SRB-CA треба да пошаље захтев за поновно дистрибуирање главног кључа који је већ успешно дистрибуиран SRB-CA, оно генерише нови захтев за дистрибуцију кључа, користећи нови генерисани краткотрајни пар кључева. Такав захтев може навести ERCA да покрене истрагу о могућности компромитације кључа.

4.2.9 Замена главног кључа новим кључем

У случају да је ERCA генерисало нову верзију главног кључа, како је наведено у Додатку 11. одељци 9.2.1.2. и 9.2.2.2, расположивост новог кључа објављује се на веб сајту ERCA, заједно са његовим бројем верзије и дужином.

Да би добио нову верзију, SRB-CA доставља нови KDR. Захтев за нови главни кључ упућује се правовремено како би се кључ (или изведени кључеви или шифровани подаци за сензоре кретања) могли на време уградити у нове компоненте.

Захтев за кључ, обрада, дистрибуција и прихватање кључа исти су као и за првобитни кључ. Произвођачи компоненти и персонализатори картица одмах се обавештавају како је даље описано у општим правилима рада SRB-CA.

4.2.10 Обавештење о компромитацији симетричног кључа

Ако SRB-CA открије или је обавештено о компромитацији или сумњи на компромитацију симетричног главног кључа, SRB-CA о томе обавештава ERCA и SRB-NA без непотребног одлагања и бар у року од 8 сати од откривања. SRB-CA у свом обавештењу наводи околности под којима је дошло до компромитације. Предузимају се истрага и могуће мере од стране SRB-NA и/или SRB-CA како је наведено у политици сертификације NA. О исходу истраге SRB-NA обавештава се ERCA.

Ако ERCA открије или је обавештено о компромитацији или сумњи на компромитацију симетричног главног кључа, ERCA о томе обавештава европско тело без непотребног одлагања и бар у року од 8 сати од откривања. Европско тело делује на одговарајући начин. ERCA поступа у складу са утврђеном процедуром поступања у случају безбедносног инцидента.

4.2.11 Услуга провере статуса главног кључа

Статус симетричних главних кључева може се преузети онлајн са https://dtc.jrc.ec.europa.eu/. ERCA одржава интегритет информација о статусу.

Информације о статусу главног кључа објављене у репозиторијуму ERCA ажурирају се првог радног дана сваке недеље.

Доступност поменутог веб сајта гарантује се за време редовног радног времена.

4.2.12 Крај претплате

Претплата за услуге дистрибуције кључева ERCA престаје када NA одлучи о престанку рада NA. NA обавештава ERCA о тој промени која представља промену националне политике.

У случају престанка претплате, MSCA безбедно уништава све копије сваког симетричног главног кључа који поседује.

4.2.13 Депоновање (escrow) и опоравак кључа

Депоновање кључева је изричито забрањено, што значи да симетрични главни кључеви никада неће бити извезени или похрањени у другом систему осим у производном и резервном систему ERCA и SRB-CA.

4.3 Захтев за сертификат и издавање сертификата тахографске картице

Више појединости о захтеву за сертификат и издавању сертификата тахографских картица може се наћи у документацији SRB-CA. Ове појединости биће достављене регистрованим персонализаторима картица.

4.3.1 Захтев за добијање сертификата

SRB-CA издаје сертификате само ако је надлежном телу достављен исправан захтев за добијање сертификата и ако су у време подношења захтева испуњени сви захтеви из Уредбе (ЕЗ) 165/2014 и свих других повезаних правних одредаба и споразума.

SRB-CA прихвата само захтеве за добијање сертификата за тахографске картице са важећим одобрењем типа, како је описано у Анексу IB (поглавље 8).

За сваку тахографску картицу генерише се један јединствени пар кључева ECC, који се назива Card_MA и који се користи за узајамну аутентификацију. Други јединствени пар кључева ECC који се назива Card_Sign (користи се за потписивање података) додатно се генерише за сваку картицу возача и сваку картицу радионице. Овај задатак могу да обављају произвођачи картица или персонализатори картица, како је описано у Анексу IB, Додатак 11. (одељак 9.1.5). Увек када се генерише пар кључева картице, страна која генерише кључ шаље јавни кључ у SRB-CA како би добила одговарајући сертификат картице који је потписало SRB-CA. Приватни кључ користи само тахографска картица. Захтеви за издавање сертификата кључева који се ослањају на транспорт приватних кључева нису дозвољени.

4.3.2 Захтеви за сертификате

Захтеви за сертификате прикупљају се у пакету захтева. Пакети се потписују помоћу приватног кључа наменске чип картице RA како је описано у SRB-CA CPS-у.

Објект податка	**Дужина**	**Формат**	**Подаци**
certificateRequestID	8 Byte	CertificateRequestID	ИД ознака захтева
cardNumber	16 Byte	CardNumber	Број картице
equipmentType	1 Byte	INTEGER	Врста уређаја: - Картица возача: '0x01' - Картица радионице: '0x02' - Контролна картица: '0x03'

			- Картица привредног друштва: '0x04' - Потпис картице возача: '0x11' - Потпис картице радионице: '0x12'
tachographApplicationID	6 Byte	ОКТЕТНИ НИЗ	Фиксно кодирана вредност (*hard coded*): 'FF 53 4D 52 44 54' („SMRDT")
PK_DP	var	Идентификатор објекта	Параметар домена; упућује на стандардизоване параметре домена који ће се користити са јавним кључем у сертификату. Он садржи један од идентификатора објекта наведених у Табели 1. Додатка 11, Анекс IB
PK_PP подаци у обичном формату Табела 4. Подаци захтева за сертификат тахографских картица	var	ОКТЕТНИ НИЗ	Јавна тачка; јавне тачке елиптичне криве конвертују се у октетне низове како је наведено у (Техничким смерницама TP03111, BSI, Криптографија елиптичних крива, V.2.0). Користи се некомпримовани формат кодирања (Анекс IB, Додатак 11, CSM_143)
потпис	var	ОКТЕТНИ НИЗ	Потпис захтева за сертификат ECC; потпис ECDSA креиран преко података захтева за сертификат у обичном формату

Табела 4. Подаци захтева за сертификат тахографских картица

Потпис се креира преко свих објеката података (у наведеном редоследу) осим „cardNumber". Алгоритам потписа је ECDSA, како је наведено у FIPS PUB 186-4, уз коришћење алгоритма хеширања повезаног са величином кључа овлашћења за потписивање. Формат потписа мора бити обичан, како је наведено у BSI/IEC 18033-2.

4.3.3 Издавање сертификата

SRB-CA се у оквиру својих овлашћења стара о томе да се изврши одговарајућа регистрација код надлежних органа пре издавања сертификата SRB-CP или произвођачу картица.

Ако се генерисање кључа одвија ван SRB-CA, SRB-CA издаје сертификат SRB-CP или произвођачу картица само ако се по унапред договореној процедури докаже да они поседују одговарајући приватни кључ. У овом тренутку приватни кључ не сме изаћи из заштићеног окружења за генерисање кључева. SRB-CA се такође стара о томе да пакет захтева за сертификат који долази од SRB-CP или произвођача картица буде потпун, тачан и прописно ауторизован. SRB-CA само у том случају издаје или потписује сертификат картице.

Провере исправности, потпуности и ауторизације врше се само на аутоматизован начин од стране система SRB-CA, како је описано у SRB-CA CPS-у. Компонента кључа за ауторизацију је чип картица RA.

SRB-CA издаје сертификат произвођачу VU само ако произвођач има пребивалиште у Европској унији. Ово се не односи на подређена друштва или производне локације произвођача.

Према Додатку 11, периоди важења сертификата CardMA су следећи:

- за картице возача: 5 година
- за картице привредног друштва: 5 година
- за контролне картице: 2 године
- за картице радионице: 1 година

Периоди важења сертификата Card_Sign су следећи:

- за картице возача: 5 година и 1 месец
- за картице радионице: 1 година и 1 месец

Датум ступања на снагу сертификата садржи датум почетка и период важења сертификата. То мора бити датум када је SRB-CA издало сертификат.

Сертификати CardMA и CardSign дате картице возача или картице радионице морају имати исти датум ступања на снагу сертификата.

Време коришћења Card_MA.SK и Card_Sign.SK мора бити исто као период важења одговарајућег сертификата.

Формат сертификата Card_MA и CardSign може се наћи у одељку 72.

4.3.4 Прихватање сертификата

SRB-CP или произвођач картица прихвата сертификат само ако се он поклапа са повезаним захтевом за сертификат и ако се сертификат може потврдити у односу на сертификат MSCACard SRB-CA који садржи MSCA_Card.PK.

4.3.5 Коришћење пара кључева и сертификата

- SRB-CP или произвођач картица бирају јачину пара кључева картице која је једнака јачини пара кључева SRB-CA који се користи за потписивање одговарајућег сертификата картице.
- Тахографска картица користи свој пар кључева Card_MA, који се састоји од приватног кључа Card_MA.SK и јавног кључа CardMA.PK, искључиво ради вршења узајамне аутентификације и усаглашавања сесијских кључева са јединицама у возилу, како је прецизирано у Анексу IB, Додатак 11.
- Картица возача или картица радионице користи CardSign приватног кључа. SK свог пара кључева CardSign искључиво за потписивање преузетих датотека са подацима, како је наведено у Додатку 11. Одговарајући CardSign јавног кључа. PK користи се искључиво за проверу потписа креираних картицом.
- Парови кључева, симетрични кључеви и бројеви пинова генеришу се и чувају у поузданом наменском уређају који:
    - има сертификацију за EAL 4 или виши у складу са ISO/IEC 15408 који користи одговарајући заштитни профил; или
    - испуњава захтеве утврђене у ISO/IEC 19790 ниво 3; или
    - испуњава захтеве утврђене у FIPS PUB 140-2 ниво 3.

Најчешћа примена таквог поузданог наменског уређаја за употребу у систему PKI је хардверски сигурносни модул (HSM)

- Операције са приватним кључем и операције са симетричним кључем одвијају се унутар HSM-а где се чувају коришћени кључеви.
- Приватни кључеви и симетрични кључеви користе се само у физички безбедном окружењу од стране особља са поузданим улогама са бар двоструком контролом. Приватни кључеви и симетрични кључеви неће се обрађивати изван HSM-а без одговарајућег шифровања. Сви догађаји коришћења приватног кључа и коришћења симетричног кључа се евидентирају.
- Парови кључева и одговарајући сертификати одређене тахографске картице не смеју се замењивати или обнављати након издавања картице.
- Издате тахографске картице садрже следеће криптографске кључеве и сертификате:
    - Приватни кључ Card_MA и одговарајући сертификат
    - За картице возача и картице радионице додатно: приватни кључ Card_Sign и одговарајући сертификат
    - Сертификат MSCACard који садржи јавни кључ MSCACard.PK који ће се користити за проверу сертификата Card_MA и сертификата Card_Sign
    - Сертификат EUR који садржи јавни кључ EUR.PK који ће се користити за проверу сертификата MSCA_Card
    - Сертификат EUR чији период важења непосредно претходи периоду важења сертификата EUR који ће се користити за проверу сертификата MSCA_Card, ако постоји.
    - Сертификат о повезаности који повезује та два сертификата EUR, ако постоји
    - Симетрични главни кључеви KM_{-WC} и KM_{-DSRC} за картице радионице
    - Симетрични главни кључ KM_{-DSRC} за контролне картице
- Поред наведених криптографских кључева и сертификата, тахографске картице такође садрже кључеве и сертификате наведене у Анексу IB, Додатак 11, Део А, чиме се тим картицама омогућава да остварују интеракцију са јединицама у возилу прве генерације.

4.3.6 Обнављање сертификата

Обнављање сертификата, тј. продужење периода важења постојећег сертификата није дозвољено.

4.3.7 Обнова сертификата са новим кључем

Обнова сертификата са новим кључем није дозвољена. Нове тахографске картице издају се по истеку важења сертификата и по истеку периода коришћења пара кључева.

4.3.8 Измена сертификата

Измена сертификата није дозвољена.

4.3.9 Опозив и суспензија сертификата

Опозив сертификата тахографских картица од стране SRB-CA није предвиђен и SRB-CA неће прихватати захтеве за опозив нити их обрађивати.

4.3.10 Услуге провере статуса сертификата

Информације о статусу сертификата за све издате сертификате тахографских картица чува SRB-CA. Ове информације се не објављују, али ће на захтев бити доступне странама са оправданим интересом.

4.3.11 Крај претплате

Претплата за услугу сертификације SRB-CA престаје када персонализатор картица или произвођач картица одлучи да прекине пружање услуге. У том случају свим издатим сертификатима тахографских картица дозвољава се да истекну. Персонализатор картица или произвођач картица обавештавају SRB-NA и SRB-CA о престанку пружања услуге. SRB-NA обавештава SRB-CIA о прекиду пружања услуге и о накнадним персонализаторима картица или произвођачима картица.

4.3.12 Депоновање (escrow) и опоравак кључева

Депоновање кључева је изричито забрањено, што значи да се приватни кључеви Card_MA.SK и Card_Sign.SK не смеју извозити или чувати на било ком другом месту осим на повезаној тахографској картици.

4.4 Захтев за добијање и издавање сертификата јединице у возилу (VU)

Није примењиво.

4.5 Захтев за добијање и издавање сертификата јединице у возилу (EGF)

Није примењиво.

4.6 Захтев за добијање симетричног главног кључа дела VU ($K_{M\text{-}VU}$), радионичког дела ($K_{M\text{-}WC}$) и главног кључа DSRC-а (K_{MDSRC}) и њихова дистрибуција

Више појединости о захтеву за добијање и дистрибуцији симетричних кључева може се наћи у документацији SRB-CA. Ове појединости биће достављене регистрованим произвођачима компоненти и персонализаторима картица.

4.6.1 Захтеви за дистрибуцију кључева

Формални захтев за дистрибуцију кључева (KDR) произвођача уређаја или персонализатора картица није неопходан. Ако се морају дистрибуирати нови симетрични кључеви, SRB-CA контактира (обично телефоном) регистровану контакт особу са приступом важећој RA-картици (како је даље наведено у Општим правилима рада SRB-CA) ради даље координације.

4.6.2 Поруке о дистрибуцији кључева

Произвођачи уређаја и персонализатори картица примају поруку о дистрибуцији кључева (KDM) као структуру података ASN.1 кодирану према DER-у, која се заснива на правилима кодирања наведеним у ISO/IEC 8825-1 као бинарну датотеку променљиве дужине:

Објект податка	**Таг**	**Дужина**	**Подаци**	**Опис**
KDM	'A1'	var		Порука о дистрибуцији кључева
CID	'5A'	18 Byte	ОКТЕТНИ НИЗ	број картице SRB-CA или одговарајуће картице RA
MRA	'83'	8 Byte		Ауторизација примаоца поруке
tacho-graphApplicati-onlD		6 Byte	,FF 53 4D 52 44 54'	6 најзначајнијих бајтова идентификатора апликације (AID)
mastertер-KeyType		1 Byte	$K_{M\text{-}WC}$ '27' $K_{M\text{-}VU}$: '67' $K_{M\text{-}SRC}$:09	Захтевана врста главног кључа (на основу дефиниција врсте опреме)
keyVerson-Number		1 Byte		Број верзије захтеваног кључа, INTEGER (0...255)
EAK	'5F 52'	var	ОКТЕТНИ НИЗ	Шифровани LKM са симетричним главним кључем, допуном PKCS#1, режим ECB (1)
S	'5F 37'	var	ОКТЕТНИ НИЗ	Потпис RA-CA преко хеш вредности главног кључа МК приложеног у LKM (2)

Табела 7. Структура KDM за дистрибуцију симетричног кључа (друге генерације) произвођачима опреме и персонализаторима картица

Напомене:

(1) Означена порука о кључу (*Labeled Key Message* - LKM) описана у наставку шифрована је јавним кључем RSA партнерске картице RA.

(2) Потпис главног кључа МК врши RA-CA (1024-битни кључ RSA, хеш вредност SHA1).

Структура LKM

Објект податка	**Таг**	**Дужина**	**Подаци**	**Опис**
LKM var	'7F 24'	var		Означена порука о кључу
CID	'5A'	18 Byte	ОКТЕТНИ НИЗ	број картице SRB-CA или одговарајуће картице RA

MRA	'83'	8 Byte		Ауторизација примаоца поруке
tacho-graphAppli-cationlD		6 Byte	,FF 53 4D 52 44 54'	6 најзначајнијих бајтова идентификатора апликације (AID)
masterKeyTyp e		1 Byte	KM-WC: '27' KM-VU: '67' KM-DSRC: '09'	Захтевана врста главног кључа (на основу дефиниција врсте уређаја)
keyVersion-Num-ber		1 Byte		Број верзије захтеваног кључа, INTEGER (0...255)
MK	'7F 51'	var		Главни кључ (16, 24 или 32 бајта)

Табела 8. Структура LKM за дистрибуцију симетричног кључа

4.6.3 Издавање симетричних основних кључева

SRB-CA се у оквиру својих овлашћења стара о томе да се изврши одговарајућа регистрација код надлежног органа пре издавања симетричних главних кључева произвођачима уређаја или персонализаторима картица. SRB-CA издаје симетричне главне кључеве произвођачима уређаја или персонализаторима картица само ако они имају пребивалиште у Европској унији. Ово се не односи на подређена друштва или производне локације произвођача уређаја или персонализатора картица.

4.6.4 Размена захтева и одговора

- За пренос порука о дистрибуцији кључа треба користити CD-R медијум или USB флеш диск (USB меморијску картицу).
- CD-R треба да буде медијум од 12 cm у режиму једне сесије (форматиран према ISO 9660:1988).
- USB флеш диск користи класу USB уређаја за масовно складиштење.
- Друге методе преноса могу се користити уз претходну сагласност SRB-CA. У сврху тестирања (само са пробним кључевима), SRB-CA шаље поруке о дистрибуцији кључева као прилоге уз електронску пошту.
- SRB-CA уписује на медијум за пренос података једну копију сваке поруке о дистрибуцији кључева за враћање произвођачу уређаја или персонализатору картица. Ова копија мора бити у бинарном формату (датотека .bin).
- Медијуме за пренос података размењују службеник и курир SRB-CA у контролисаном подручју SRB-CA.

4.6.5 Прихватање кључа

- Курир потписује пријем поруке о дистрибуцији кључева у просторијама SRB-CA. По пријему поруке о дистрибуцији кључева у просторијама произвођача уређаја или персонализатора картица, партнер проверава следеће:

  о да ли је медијум за пренос података читљив, тј. да није оштећен или неисправан;

  о да ли је формат поруке је у складу са структуром описаном у одељку 4.6.2;

- о да ли врста и верзија кључа у поруци одговарају захтеваној врсти и верзији.

- Ако су све ове провере успешне, партнер дешифрује симетрични кључ како је наведено у одељку 4.6.2, користећи одговарајућу картицу RA.
- Дешифровање симетричног кључа одвија се само у HSM-у који испуњава захтеве из одељка 6.2.

4.6.6 Коришћење кључа

Произвођачи уређаја или персонализатори картица користе сваки примљени симетрични кључ у складу са одељком 6.2.

4.6.7 Обнављање KDM

Обнављање KDM, тј. издавање копије постојеће KDM произвођачу уређаја или персонализатору картица није дозвољено. У случају да је оригинални медијум за пренос података који је примио произвођач уређаја или персонализатор картица оштећен или неисправан, мора се генерисати нова KDM.

4.6.8 Замена кључа новим кључем

У случају да је ERCA генерисало нову верзију симетричног главног кључа, како је наведено у Додатку 11. одељ. 9.2.1.2. и 9.2.2.2, SRB-CA обавештава произвођаче уређаја или персонализаторе картица о доступности новог симетричног кључа ради даље координације. Захтев за кључ, обрада, дистрибуција и прихватање кључа исти су као и за првобитни кључ. Дистрибуирање нових симетричних кључева врши се правовремено како би се кључ (или изведени кључеви или шифровани подаци за сензоре кретања) могли на време уградити у нове компоненте.

4.6.9 Обавештење о компромитацији симетричног кључа

Ако произвођач компоненти или персонализатор картица открије или је обавештен о компромитацији или сумњи на компромитацију симетричног главног кључа, произвођач компоненти или персонализатор картица о томе обавештавају SRB-CA и SRB-NA без непотребног одлагања и бар у року од 8 сати од откривања. Произвођач компоненти или персонализатор картица у свом обавештењу наводе околности под којима је дошло до компромитације. Произвођач компоненти или персонализатор картица поступају у складу са утврђеном процедуром поступања у случају безбедносног инцидента. Након инцидента, резултати накнадне истраге, почетних и могућих мера пријављују се SRB-CA и SRB-NA први пут најкасније недељу дана након откривања инцидента.

Поред хитних мера које предузимају произвођач компоненти или персонализатор картица, SRB-CA и SRB-NA проверавају и усаглашавају одговарајуће мере које могу укључивати привремен или коначан прекид услуга које SRB-CA нуди погођеном произвођачу компоненти или персонализатору картица. Све мере које SRB-CA и SRB-NA предузму биће координисане са ERCA и инцидент ће бити пријављен у што краћем року, али најкасније 8 сати од откривања или обавештења.

Ако се безбедносни инцидент догоди у SRB-CA, SRB-CA ће поступити како је описано. SRB-NA, ERCA и евентуално погођени произвођачи компоненти или персонализатори картица биће обавештени одмах, а најкасније 8 сати од откривања инцидента.

Компромитација симетричног кључа сматра се озбиљним безбедносним инцидентом је разлог за ванредну ревизију према одељку 8.1, која се фокусира на радње повезане са инцидентом.

4.6.10 Услуга провере статуса кључа

SRB-CA не објављује нити посебно пружа услугу провере статуса за симетричне кључеве.

4.6.11 Крај претплате

Претплата на услуге дистрибуције кључева престаје када произвођач уређаја или персонализатор картица одлучи да прекине своју услугу. О таквој промени произвођачи уређаја или персонализатори картица обавештавају SRB-CA.

У случају престанка претплате, произвођачи уређаја или персонализатори картица безбедно уништавају све копије сваког симетричног кључа који поседују.

4.6.12 Депоновање (escrow) и опоравак кључа

Депоновање кључева је изричито забрањено, што значи да симетрични кључеви неће бити извезени или похрањени у неком другом систему осим у системима произвођача уређаја или персонализатора картица.

4.7 Услуге шифровања SRB-CA за кључ за упаривање и серијске бројеве сензора кретања и за генерисање симетричних кључева DSRC-а $K\_VU_{DSRC}\_ENC$ и $K\_VU_{DSRC}\_MAC$ специфичних за дату VU

Није примењиво.

5 Контрола објекта, управљања и функционисања

5.1 Физичке контроле

- Услуге генерисања кључева и сертификата SRB-CA и одговарајуће услуге произвођача компоненти и персонализатора картица смештене су у безбедном простору, са означеним зонама безбедности, одговарајућим безбедносним баријерама и контролом уласка ради спречавања неовлашћеног приступа, оштећења и ометања. Овај простор надгледају радници обезбеђења и морају се поставити сигурносни аларми.
- Напајање електричном енергијом и климатизација за системе SRB-CA морају бити одговарајући и потребно је успоставити редундантност.
- Системи и медијуми за складиштење поверљивих информација SRB-CA, произвођача компоненти и персонализатора картица, као што су чврсти дискови, паметне картице и HSM-ови, заштићени су од неовлашћене или ненамерне употребе, приступа, обелодањивања или оштећења од стране људи или од других претњи (нпр. пожар, поплава).
- Медијуми за чување резервних копија и за инсталацију чувају се на посебној локацији која је физички обезбеђена и заштићена од неовлашћене или ненамерне употребе, приступа, обелодањивања, оштећења од стране људи или од других претњи (нпр. пожар, поплава).
- Примењују се поступци за одлагање отпада како би се избегла неовлашћена употреба, приступ или обелодањивања поверљивих података.
- За складиштење критичних података SRB-CA и података потребних за хитан опоравак користи се место изван локације објекта.

5.2 Процедуралне контроле

- SRB-CA, произвођачи компоненти и персонализатори картица спроводе процедуралне контроле како би се обезбедио безбедан рад. Нарочито се врши раздвајање дужности спровођењем контроле од стране више особа за критичне задатке.
- Приступ системима SRB-CA и одговарајућим системима произвођача компоненти и персонализатора картица ограничен је на појединце који су прописно ауторизовани и имају приступ само на основу потребе за добијањем информација. Нарочито се уводе следеће мере контроле приступа:
    - поверљиви подаци штите се ради заштите интегритета и поверљивости похрањених података;
    - поверљиви подаци штите се ради заштите интегритета и поверљивости похрањених података;
    - поверљиви подаци који се бришу уништавају се трајно, нпр. уписивањем насумичних података преко њих више пута, користећи безбедни метод који признаје BSI.
    - Системи SRB-CA и одговарајући системи произвођача компоненти и персонализатора картица обезбеђују делотворну администрацију корисника и управљање приступом;

  - Системи SRB-CA и одговарајући системи произвођача компоненти и персонализатора картица обезбеђују да приступ функцијама система за информисање и подношење захтева буде ограничен на овлашћено особље и обезбеђују довољну контролу рачунарске безбедности за раздвајање поузданих улога. Конкретно, употреба системских корисничких програма ограничена је и строго контролисана. Приступ је ограничен и приступ ресурсима дозвољава се само ако је то неопходно за обављање улоге додељене кориснику;
  - SRB-CA и повезани произвођачи компоненти и персонализатори картица идентификују се и аутентификују пре коришћења система SRB-CA или одговарајућих система произвођача компоненти и персонализатора картица.
  - Особље SRB-CA, произвођача компоненти и персонализатора картица одговорно је за своје активности, које се евидентирају у дневнику догађаја како је описано у одељку 5.4;
- SRB-CA, произвођачи компоненти и персонализатори картица успостављају систем управљања информационом безбедношћу (ISMS) на основу процене ризика за све укључене операције. Они обезбеђују да политике ISMS решавају питања обуке особља, одобрења и улога. Спровођење ISMS треба да испуњава захтеве описане у ISO 27001.

5.3 Контроле особља

- Обавезе SRB-CA могу се поверити спољном специјализованом привредном друштву или се за извршавање обавеза SRB-CA може ангажовати особље извођача.
- Сво особље укључено у рад SRB-CA или повезано особље произвођача компоненти и персонализатора картица мора бити адекватно обучено и поседовати стручно знање, искуство и квалификације неопходне за понуђене услуге и одговарајуће за радно место. Ово се односи на особље које је директно запослено, особље из специјализованог привредног друштва коме су задаци поверени или особље извођача.
- Обука особља одвија се према плану обуке описаном у одговарајућем CPS-у или концепту безбедности.
- Именовањем особља за поуздане улоге управља се у складу са поступком скрининга утврђеним у CPS-у или концепту безбедности.
- Поуздане улоге од којих зависи безбедност операције јасно су утврђене у одговарајућем CPS-у или концепту безбедности. Ове улоге и повезане обавезе документују се у концепту улога или упоредивом документу. Овај концепт улога утврђује се са становишта раздвајања дужности и најмање привилегија. Ниједна особа не може бити овлашћена да истовремено обавља више од једне поуздане улоге.

5.4 Поступци евидентирања у ревизорским дневницима

Сви значајни безбедносни догађаји у софтверу SRB-CA или повезаном софтверу произвођача компоненти и персонализатора картица аутоматски добијају временски жиг и евидентирају се у системским датотекама евиденције. То укључује најмање следеће:

- успешне и неуспешне покушаје да се креирају, ажурирају, уклоне или преузму информације о статусу налога особља или да се поставе или укину привилегије налога;
- успешне и неуспешне покушаје да се подеси или промени начин аутентификације (нпр. лозинка, биометријски, криптографски сертификат) повезан са личним налогом;
- успешне и неуспешне покушаје пријављивања на налог и одјављивања са налога;
- успешне и неуспешне покушаје промене конфигурације софтвера;
- покретања и заустављања софтвера;
- ажурирања софтвера;
- покретање и гашење система;
- успешне и неуспешне покушаје додавања или брисања субјекта из регистра претплатника којима SRB-CA тренутно пружа услуге сертификације кључа, мењања података за било ког претплатника или преузимања информација из регистра;
- успешне и неуспешне покушаје обраде захтева за потпис сертификата или захтева за дистрибуцију кључа;
- успешне и неуспешне покушаје потписа сертификата или генерисања поруке о дистрибуцији кључа;
- успешне и неуспешне интеракције са базама података које садрже податке о издатим сертификатима (статусу издатих сертификата), укључујући покушаје повезивања и операције читања, писања и ажурирања или уклањања;
- успешне и неуспешне покушаје повезивања на HSM или искључивања са HSM-а;
- успешне и неуспешне покушаје аутентификације корисника на HSM;
- успешне и неуспешне покушаје да се генерише или уништи пар кључева или симетрични кључ у HSM-у;
- успешне и неуспешне покушаје увоза кључа у HSM или извоза кључа из HSM-а;
- успешне и неуспешне покушаје промене стања животног циклуса пара кључева или симетричног кључа;
- успешне и неуспешне покушаје коришћења приватног кључа или симетричног кључа унутар HSM-а у било коју сврху.

Да би се могли испитати безбедносни инциденти, ако је то могуће, системски дневник садржи информације које омогућавају идентификацију особе или налога који је извршио системске задатке. Интегритет евиденције дневника догађаја у систему одржава се и штити од неовлашћених прегледа, модификације, брисања или уништења. Прави се резервна копија дневнике догађаја у систему и интерно се похрањује.

5.5 Архивирање евиденције

- Преглед догађаја који се архивирају описује се у интерним поступцима и у складу је са релевантним правилима и прописима. SRB-CA, произвођачи компоненти и персонализатори картица примењују одговарајуће поступке архивирања евиденције. Успостављају се процедуре за обезбеђивање интегритета, аутентичности и поверљивости евиденције.

- Све архивиране информације архивирају се на неограничено време.
- Предузимају се мере да се архива евиденције чува тако да је губитак оправдано искључен.
- Интегритет догађаја поменутих у одељку 5.4. периодично се проверава. Ови инспекцијски прегледи обављају се бар једном годишње.

5.6 Замена кључева

- SRB-CA по потреби генерише нове парове кључева SRB-CA. Након што SRB-CA генерише нови пар кључева, он подноси захтев за обнову сертификата са новим кључем како је описано у одговарајућем одељку политике ERCA и дистрибуира кључеве персонализаторима компоненти SRB-CP како је описано у одељцима о замени кључа новим кључем у поглављу 4. ове политике.
- SRB-CA обезбеђује да се заменски кључеви генеришу у контролисаним околностима и у складу са поступцима утврђеним у овој политици сертификације.

5.7 Опоравак од компромитације и катастрофалног догађаја

SRB-CA, произвођачи компоненти и персонализатори картица утврђују процедуре поступања у случају безбедносних инцидената и компромитације у Приручнику о процедурама поступања у случају безбедносних инцидената, који се издаје администраторима и ревизорима.

SRB-CA, произвођачи компоненти и персонализатори картица имају спреман План за континуитет пословања који прецизира како ће они пружати своје услуге у случају инцидента који утиче на редован рад. По откривању инцидента, операције се обустављају док се не утврди ниво компромитације. Осим тога, SRB-CA, произвођачи компоненти и персонализатори картица претпостављају да ће због технолошког напретка њихови ИТ системи временом постати застарели. Мере за управљање застарелошћу утврђују се у Плану за континуитет пословања.

Процедуре прављења резервних копија и опоравка за све релевантне податке описане су у Плану прављења резервних копија и опоравка.

Катастрофалним догађајем сматрају се следећи инциденти:

- компромитација или крађа приватног кључа (SRB-CA_Card.SK,) и/или симетричног главног кључа ($K_{M\text{-}WC}$,
- губитак приватног кључа (SRB-CA_Card.

  SK,) и/или симетричног главног кључа ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$)
- Квар ИТ хардвера.

У случају компромитације или крађе приватног кључа SRB-CA који се користи за потписивање сертификата јавног кључа тахографских картица (SRB-CA_Card.

SK), SRB-CA одмах обавештава SRB-NA, SRB-CIA, погођене персонализаторе компоненти SRB-CP и ERCA. Све погођене стране предузимају одговарајуће мере у разумном року.

У случају компромитације или крађе једног или више симетричних главних кључева које чува SRB-CA, SRB-CA одмах обавештава SRB-NA, ERCA и погођене персонализаторе компоненти. Све погођене стране предузимају одговарајуће мере у разумном року.

Ефективно нема опоравка од губитка приватних кључева или симетричних главних кључева SRB-CA. Губитак се стога спречава коришћењем вишеструких резервних копија одговарајућих кључева и главних кључева, који се периодично контролишу.

Заштита од кварова на ИТ хардверу обезбеђује се редундантношћу, тј. расположивошћу дуплираног ИТ хардвера.

Ови механизми не зависе од времена реакције ERCA.

5.8 Престанак пружања услуга

У случају прекида делатности SRB-CA од стране именоване организације, SRB-NA о томе обавештава EA и ERCA а необавезно обавештава EA и ERCA о новоименованом SRB-CA. SRB-NA обезбеђује да најмање један SRB-CA буде у функцији у сваком тренутку.

Ако произвођач компоненти прекине своју делатност, о томе се обавештава SRB-CA. SRB-CA затим обавештава SRB-NA а SRB-NA необавезно обавештава EA и ERCA.

У случају прекида услуге персонализатора картица, SRB-CA, SRB-NA и CIA обавештавају се о томе, а SRB-NA необавезно обавештава EA и ERCA. SRB-NA обезбеђује да најмање један персонализатор картица буде у функцији у сваком тренутку. SRB-NA обавештава CIA, EA и ERCA о новоименованом персонализатору картица.

6 Техничке безбедносне контроле

6.1 Генерисање и инсталација пара кључева

- SRB-CA, произвођачи компоненти и персонализатори картица генеришу приватне кључеве у складу са Анексом IB, Додатак 11.
- Генерисање и уметање парова кључева и главних кључева спроводи се у физички обезбеђеном окружењу од стране особља у поузданим улогама под контролом најмање две особе. Церемонија генерисања кључева се документује.
- SRB-CA мора имати на располагању систем SRB-CA за тестирање за потребе испитивања интероперабилности, у складу са Уредбом. Систем SRB-CA за тестирање је одвојен систем и има сопствене приватне кључеве и симетричне главне кључеве SRB-CA. Систем SRB-CA за тестирање мора бити у могућности и да захтева потпис пробних сертификата и дистрибуцију симетричних пробних кључева користећи процесе описане у овом документу и политици ERCA. SRB-CA за тестирање такође мора бити у могућности да потпише пробне сертификате за уређаје на захтев персонализатора компоненти и да дистрибуира симетричне пробне кључеве и шифроване податке за сензоре кретања персонализаторима компоненти.

6.2 Заштита приватног кључа и техничке контроле криптографског модула

SRB-CA, произвођачи компоненти и персонализатори картица чувају поверљивост, интегритет и доступност приватних и симетричних кључева како је описано у овом одељку.

Приватни кључеви и симетрични кључеви генеришу се и чувају у поузданом наменском уређају који:

- сертификован је за EAL 4 или виши у складу са ISO/IEC 15408 који користи одговарајући заштитни профил; или
- испуњава захтеве утврђене у ISO/IEC 19790 ниво 3; или
- испуњава захтеве утврђене у FIPS PUB 140-2 ниво 3; или
- нуди еквивалентан ниво сигурности према еквивалентним националним или међународно признатим критеријумима за оцену ИТ безбедности.

Најчешћа примена таквог поузданог наменског уређаја за употребу у систему PKI је хардверски сигурносни модул (HSM). Могуће су и друге примене уз коришћење различитих уређаја, све док усвојени уређаји задовољавају један од наведених безбедносних захтева. Поред тога, осим ових безбедносних захтева, ова политика сертификације SRB-NA садржи различите функционалне захтеве за поуздан наменски уређај који се користи у систему SRB-CA. Напомиње се да у случају коришћења другог уређаја уместо HSM-а, сви ти функционални захтеви такође морају бити испуњени. Термин „HSM” се у овом документу користи као скраћеница за овде наведене захтеве.

Операције са приватним кључем и операције са симетричним кључем одвијају се интерно у HSM-у где се чувају коришћени кључеви.

Приватни кључеви и симетрични кључеви SRB-CA, произвођача компоненти и персонализатора картица користе се само у физички безбедном окружењу од стране особља у поузданим улогама са бар двоструком контролом. Сви догађаји коришћења приватног кључа и коришћења симетричног главног кључа се евидентирају.

Резервне копије приватних кључева и симетричних кључева SRB-CA, произвођача компоненти и персонализатора картица прави, чува и опоравља само особље у поузданим улогама са контролом бар две особе у физички обезбеђеном окружењу.

За резервне копије приватних кључева и симетричних кључева SRB-CA, произвођача компоненти и персонализатора картица важи исти ниво безбедносних контрола као и за кључеве који су у употреби.

Једна резервна копија сваког приватног кључа и сваког главног кључа SRB-CA чува се изан локације објекта.

Увоз и извоз приватног кључа одвија се само у сврху прављења резервних копија и преузимања.

Увоз и извоз симетричног кључа дозвољени су за прављење резервних копија и преузимање. За SRB-CA, извоз $K_{M\text{-}WC}$ и кључева специфичних за дату VU за DSRC дозвољен је у шифрованом облику као одговор на важећи захтев за дистрибуцију кључа од персонализатора компоненти, од стране особља у поузданим улогама са контролом бар две особе.

Увоз и извоз главног кључа из сваког другог разлога је забрањен.

На крају животног циклуса приватног кључа или симетричног кључа SRB-CA (како је наведено у SRB-CA CPS), све копије кључа уништавају се тако да се не могу повратити.

Приватни кључеви и симетрични кључеви деактивирају се и уништавају ако постоји сумња на компромитацију. Кључеви се уништавају након што се испита компромитација и донесе одлука да се кључ деактивира.

Уништавање приватних кључева и главних кључева обавља се коришћењем функције HSM-а за уништавање кључева. Уништавају се и резервне копије компромитованих кључева.

6.3 Други аспекти управљања паровима кључева

Сертификати јавног кључа SRB-CA, а тиме и јавни кључеви, архивирају се на неодређено време.

Период важења свих сертификата SRB-CA у складу је са Анексом IB, Додатак 1.

У складу са Анексом IB, Додатак 11, период коришћења приватних кључева SRB-CA је две године. Период коришћења приватног кључа почиње на датум ступања на снагу

наведен у одговарајућем сертификату. SRB-CA не може користити приватни кључ након истека његовог периода коришћења.

6.4 Подаци о активацији

Приватни кључеви и/или симетрични главни кључеви SRB-CA ускладиштени у HSM-у активирају се за коришћење ако су се све особе које контролишу кључ аутентификовале према HSM-у. Аутентификација се одвија коришћењем одговарајућих средстава (нпр. приступних фраза, токена за аутентификацију).

Сесија аутентификације не траје неограничено.

За активацију самог софтвера SRB-CA, аутентификација корисника врши се коришћењем одговарајућих средстава (нпр. приступном фразом).

6.5 Безбедносне контроле рачунара

SRB-CA, произвођачи компоненти и персонализатори картица прецизирају и одобравају поступке и конкретне техничке мере безбедности за управљање својим рачунарским системима. Ови поступци гарантују да је захтевани ниво безбедности увек испуњен. Поступци и техничке мере безбедности описане су у интерној документацији и/или безбедносним концептима. Рачунарски системи организовани су и њима се управља у складу са овим поступцима, поступцима наведеним у безбедносним концептима и поступцима најбоље праксе за центре поверења и за поуздано рачунарство.

6.6 Животни циклус безбедносних контрола

SRB-CA, произвођачи компоненти и персонализатори картица спроводе анализу безбедносних захтева у фази пројектовања и прецизирања захтева ради уграђивања безбедности у њихове системе.

Систем прихватања (или предпроизводни систем) и производни систем остају раздвојени. Поступци за вршење промена и поступци управљања безбедношћу гарантују да се у производном систему одржава захтевани ниво безбедности.

Поступци за контролу вршења промена документују се и користе за издавање, модификације и (хитне) поправке софтвера за све оперативне софтвере.

6.7 Безбедносне контроле рачунарске мреже

SRB-CA, произвођачи компоненти и персонализатори картица осмишљавају и имплементирају своју архитектуру мреже тако да се приступ њиховом домену интерне мреже са интернета и приступ са домена интерне мреже системима сертификационог тела и повезаним системима произвођача компоненти и персонализатора картица може делотворно контролисати.

6.8 Временски жиг

Време и датум догађаја садржани су у сваком уносу у ревизорски траг. SRB-CA CPS и одговарајућа документација / CPS произвођача компоненти и персонализатора картица описују како се синхронизује и верификује време.

7 Профили сертификата, CRL и OCSP

7.1 Профил сертификата

Сви сертификати морају имати профил прецизиран у Анексу IB, Додатак 11. и Додатак 1:

Објект податка	Req	Идентификациона ознака поља	Таг	Дужина (у бајтовима)	Врста података ASN.1
Сертификат ECC (CV)	m	C	'7F 21'	var	
Тело сертификата	m	B	'7F 4E'	var	
Идентификатор профила сертификата	m	CPI	'5F 29'	'01'	INTEGER (0...255)
Референтна ознака сертификационог тела	m	CAR	'42'	'08'	KeyIdentifier
Ауторизација имаоца сертификата	m	CHA	'5F 4C'	'07'	Ималац сертификата Ауторизација
Јавни кључ	m	PK	'7F 49'	var	
Стандардизовани параметри домена OID	m	DP	'06'	var	ИДЕНТИФИКАТОР ОБЈЕКТА
Јавна тачка	m	PP	'86'	var	ОКТЕТНИ НИЗ
Референтна ознака имаоца сертификата	m	CHR	'5F 20'	'08'	KeyIdentifier
Датум ступања на снагу сертификата	m	CEfD	'5F 25'	'04'	TimeReal
Датум истека важења сертификата	m	CExD	'5F 24'	'04'	TimeReal
Потпис сертификата ECC	m	S	'5F 37'	var	ОКТЕТНИ НИЗ

Табела 9. Профил

Алгоритам је назначен преко стандардизованих параметара домена OID како је наведено у Табели 1. Додатка 11, Анекс 1B. Опције су следеће:

Назив	Референтна ознака идентификатора објекта	Вредност идентификатора објекта
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
BrainpoolP384r1	BrainpoolP384r1	1.3.36.3.3.2.8.1.1.11

Табела 10. Дозвољени стандардизовани параметри домена

7.2 Профил CRL

CRL се не објављује. Статус свих издатих сертификата за ERCA може се наћи на веб сајту https://dtc.jrc.ec.europa.eu/

7.3 Профил OCSP

OCSP се не користи.

8 Ревизија усаглашености и друга оцењивања

8.1 Учесталост или околности за оцењивање

- Потпуна и формална ревизија рада SRB-CA и рада произвођача компоненти и персонализатора картица спроводи се по налогу SRB-NA. Ревизијом се утврђује да ли су и даље испуњени захтеви из ове политике сертификације и политике ERCA. SRB-NA спроводи прву ревизију у року од 12 месеци од почетка операција обухваћених одобреном политиком сертификације SRB-NA.
- Пре почетка операција обухваћених политиком сертификације SRB-NA, SRB-NA врши предоперативну процену како би добило доказе да је организација у стању да ради у складу са захтевима политике сертификације SRB-NA.
- Ако се ревизијом не добију докази о неусаглашености, следећа провера врши се у року од 12 до 24 месеца. Ако се ревизијом утврде докази о неусаглашености, накнадна ревизија врши се у року од 12 месеци да би се проверило да ли су неусаглашености отклоњене.
- У случају озбиљног безбедносног инцидента ванредна ревизија врши се у року од 6 месеци од откривања инцидента. Озбиљни инциденти у овом контексту су посебно губитак интегритета или поверљивости приватних и/или симетричних кључева. Ова ревизија фокусира се на околности и мере праћења у вези са инцидентом. Ванредна ревизија након безбедносног инцидента неће утицати на учесталост редовне ревизије како је описано у одељку 8.1.
- SRB-NA извештава ERCA о резултатима ревизије и доставља извештаје о ревизији на енглеском језику. У извештајима о ревизији утврђују се све корективне мере потребне за испуњавање обавеза SRB-NA, укључујући распоред њихове примене.

8.2 Идентитет / стручне квалификације оцењивача

- Ревизију врши независни ревизор.
- Свако лице изабрано или предложено да врши ревизију усаглашености SRB-CA, произвођача компоненти или персонализатора картица претходно мора добити одобрење SRB-NA.
- Имена ревизора који ће вршити ревизије морају се регистровати. Ти ревизори морају испуњавати следеће захтеве:
  - Етичко понашање – веродостојност, једнообразност и поверљивост у погледу њиховог односа са странама које се проверавају и приликом поступања са информацијама и подацима тих страна;
  - Правично представљање - налази, закључци и извештаји ревизије морају бити истинити и прецизно описивати све активности спроведене током ревизије;
  - Професионални приступ – ревизор има висок ниво стручног знања и стручне оспособљености и ефикасно користи своје искуство стечено кроз добру праксу дубоко укорењену у информационим технологијама, PKI и повезаним техничким нормама и стандардима.
  - Добра репутација - у SRB-NA се мора доставити сертификат о примереном понашању.

- Ревизор мора поседовати значајно знање и пожељно је да буде акредитован за:
  - спровођење ревизије безбедности информационог система;
  - PKI и криптографских технологија;
  - функционисање софтвера PKI;
  - релевантне политике и прописе Европске комисије.

8.3 Однос оцењивача према оцењиваном субјекту

- Ревизор је независан и није повезан са SRB-CA, произвођачем компоненти или персонализатором картица.

8.4 Области обухваћене оцењивањем

- Ревизија SRB-CA, произвођача компоненти или персонализатора картица обухвата усаглашеност са политиком ERCA, политиком сертификације SRB-NA, SRB-CA CPS-ом и CPS-ом или сличним документима произвођача компоненти или персонализатора картица за паметне тахографе 2. генерације, као и повезане поступке и технике које су документовали SRB-CA или произвођачи компоненти и персонализатори картица.
- Предмет ревизије усаглашености је спровођење техничких, процедуралних и кадровских пракси описаних у овим документима. Неке од приоритетних области ревизија су следеће области:
  - идентификација и аутентификација
  - оперативне функције/услуге;
  - контроле физичке и процедуралне безбедности и безбедности особља;
  - контроле техничке безбедности;
  - процедуре поступања у случају безбедносних инцидената.
- Оцењивањем ревизорских дневника утврђује се да ли постоје слабости у безбедности система SRB-CA или произвођача компоненти и персонализатора картица. Ублажавају се (евентуалне) утврђене слабости. Оцена и евентуалне слабости се евидентирају.
- У случају ванредне ревизије због тешког безбедносног инцидента, ревизија се фокусира на процесе и техничке мере у погледу тог безбедносног инцидента.

8.5 Мере предузете на основу утврђених недостатака

Ако ревизор открије недостатке који су узрок неусаглашености, SRB-CA, произвођачи компоненти или персонализатори картица одмах предузимају корективне мере. Након спровођења корективних мера, накнадна ревизија врши се у року од 12 месеци.

8.6 Достављање резултата

Независни ревизор доставља комплетне резултате ревизије усаглашености на српском и енглеском језику субјекту ревизије (SRB-CA, произвођач компоненти или персонализатор картице) и SRB-NA. SRB-NA упућује ERCA извештај о ревизији за SRB-CA који обухвата релевантне резултате ревизије. То укључује бар број пронађених одступања и природу сваког одступања. Датум пријема извештаја о ревизији објављује се на веб сајту ERCA.

Ако то затражи ERCA, SRB-NA шаље комплетне резултате ревизије усаглашености свих проверених субјеката.

9 Остала пословна и правна питања

9.1 Накнаде

Накнаде за симетричне кључеве, услуге шифровања и сертификате обрачунавају се искључиво на основу стварних трошкова за пружање потребних услуга од стране SRB-CA.

9.2 Финансијска одговорност

Нема захтева.

9.3 Поверљивост пословних информација

Поверљиви подаци обухватају:

- податке о личности (нпр. запослених у SRB-CA, произвођача компоненти или представника ERCA);
- приватне кључеве;
- симетричне главне кључеве;
- податке о привредном друштву или производњи;
- разлоге за опозив сертификата;
- ревизорске дневнике (осим ако се приступ не захтева законом, прописима или одредбама CP или CPS);
- детаљну документацију у вези са управљањем PKI;
- извештаје о ревизији интерних или екстерних ревизора.

Поверљиве информације неће бити објављене, осим ако за то не постоји законска обавеза.

9.4 Приватност података о личности

Једини подаци о личности који се обрађују или чувају у систему SRB-CA су подаци о ERCA, SRB-CA и представницима персонализатора компоненти

Ови подаци третирају се у складу са Општом уредбом о заштити података о личности 2016/679.

9.5 Права интелектуалне својине

SRB-CA поседује свеобухватна имовинска права за софтвер SRB-CA како је дефинисано у одговарајућим уговорима.

9.6 Изјаве и гаранције

SRB-CA делује у складу са ERCA CP, овом CP и сопственим CPS.

9.7 Одрицања од гаранција

SRB-CA се одриче гаранција и обавеза сваке врсте, укључујући све гаранције за тржишна својства, све гаранције за погодност за одређену намену и све гаранције за тачност пружених информација (осим ако не долазе из овлашћеног извора) и даље се одриче сваке и свих одговорности за немар и недостатак разумне пажње од стране претплатника и трећих страна.

9.8 Ограничења одговорности

Република Србија није одговорна за губитак:

- услуге због рата, природних катастрофа или других сила које се не могу контролисати;
- настао између времена промене статуса сертификата и следеће заказане објаве информација о статусу сертификата;
- због неовлашћене употребе сертификата које је издало SRB-CA и употребе сертификата мимо прописане употребе утврђене овом политиком сертификације и Општим правилима рада SRB-CA;
- узрокован преварним или немарним коришћењем сертификата и/или информација о статусу сертификата које је издало SRB-CA.

Република Србија одриче се одговорности сваке врсте за сваку накнаду, штету или друго потраживање или обавезу било које врсте које проистичу из деликтне одговорности, уговора или из било ког другог разлога у вези са услугом повезаном са издавањем, коришћењем или ослањањем на:

- сертификат који је издало SRB-CA, или његов повезани пар јавних/приватних кључева, који користи претплатник или трећа страна;
- симетрични кључ који дистрибуира SRB-CA, који користи претплатник или трећа страна;
- симетрични кључ који дистрибуира SRB-CA, који користи претплатник или трећа страна;

Издавање сертификата, симетричних кључева и услуга шифровања од стране SRB-CA не чини Републику Србију или SRB-CA заступником, фидуцијаром, повереником или другим представником подносилаца захтева, трећих страна или других лица која користе систем управљања кључевима паметног тахографа.

Претплатници и треће стране не квалификују се за захтеве за обештећење за губитке настале због неодговарајућег или преварног коришћења овог система управљања кључевима.

Поред тога, SRB-CA није посредник у трансакцијама између претплатника и трећих страна. Одштетни захтеви против SRB-CA ограничени су на доказивање да је SRB-CA функционисало на начин који није у складу са овом политиком сертификације и SRB-CA CPS-ом.

9.9 Одштета

Нема захтева.

9.10 Период важења и престанак важења

Ова политика сертификације SRB-NA важи од почетка функционисања SRB-NA. Период важења није временски ограничен.

Важење ове CP престаје са престанком пословања SRB-CA или када SRB-CA објави да ова CP више није важећа, нпр. јер ступа на снагу њена нова верзија.

9.11 Појединачна обавештења и комуникација са учесницима

Службена обавештења и комуникација са учесницима у систему управљања кључевима паметног тахографа одвијају се у писаном облику и подлежу поступцима регистрације комуникације који су на снази у Европској комисији.

Обавештење о раздвајању или спајању може довести до промена у обиму, управљању и/или функционисању DCA. У том случају могу бити потребне и измене ове политике сертификације SRB-NA и SRB-CA CPS. Промене у овим документима врше се на начин који је у складу са административним захтевима наведеним у одељку 9.12. овог документа.

9.12 Измене

Ова CP објављује се под одговорношћу SRB-NA. SRB-NA може ревидирати ову CP ако сматра да је то неопходно.

Поступак за предлоге измена и одобрења ове CP је следећи:

1. Коментари или захтеви за измену CP упућују се SRB-NA. Та комуникација обухвата опис коментара или захтеване промене, образложење и контакт податке о особи која доставља коментаре или захтева измену.

2. SRB-CA прихвата, прихвата са изменама или одбија коментар или предложену измену након завршетка периода предвиђеног за достављање коментара. SRB-NA разматра диспозицију предложених измена SRB-CA. Одлуке у погледу предложених измена су дискрециono право SRB-CA и SRB-NA.

3. ERCA одобрава нову верзију ове CP или њеног еквивалента, као и све неуредничке измене политике, осим промене CA/CP. Нова верзија ове CP биће објављена на веб сајту SRB-NA након што је одобри ERCA.

Сваку промену ове CP прати верзија документа која носи већи број. Једине промене које се могу извршити у CP и CPS-у без промене броја верзије документа су уредничке или типографске исправке.

SRB-CA може променити контакт податке из одељка 1.5. уз обавештавање SRB-NA и ERCA, али без промене броја верзије документа. Све остале измене CP врше се у складу са поступком измене наведеном у овом одељку.

9.13 Одредбе о решавању спорова

Сваки спор у вези са управљањем кључевима и сертификатима за систем дигиталног тахографа настао између DCA и организације или појединца изван Европске комисије решава се коришћењем одговарајућег механизма за решавање спорова. Спор се, по могућности, решава преговорима. Спор који није решен преговорима треба решити арбитражом европског тела.

9.14 Меродавно право

Српски и европски прописи регулишу извршивост, грађу, тумачење и ваљаност ове политике сертификације SRB-NA.

9.15 Усаглашеност са важећим правом

Ова политика сертификације у складу је са Уредбом (ЕУ) број 165/2014 Европског парламента и Савета и Спроведбеном уредбом Комисије (ЕУ) 2016/799. У случају неслагања између овог документа и Уредбе или Спроведбене уредбе, предност има потоња.

9.16 Разне одредбе

Нема захтева.

9.17 Остале одредбе

Нема захтева.

10 Упућивања

1. Уредба (ЕУ) број 165/2014 Европског парламента и Савета од 4. фебруара 2014. године, Службени лист Европске уније L60
2. Спроведбена уредба Комисије (ЕУ) 2016/799, Службени лист Европске уније L139
3. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Политика сертификације инфраструктуре јавних кључева и оквир практичних правила сертификације), новембар 2003. године.
4. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels (Кључне речи за коришћење у RFC за приказивање нивоа захтева), март 1997. године
5. ETSI EN 319 411-1, Електронски потписи и инфраструктуре (ESI); Захтеви у погледу политике и безбедности за пружаоце услуга од поверења који издају сертификате; Део 1: Општи захтеви, верзија 1.1.1, 02.2016.
6. ETSI TS 102 042, Електронски потписи и инфраструктуре (ESI); Захтеви у погледу политике за сертификациона тела која издају сертификате јавног кључа, верзија 2.4.1, 02.2013.
7. Паметни тахограф – Општа правила сертификације ERCA, JRC, верзија 1.0, месец година
8. Паметни тахограф – Спецификација испитивања интероперабилности уређаја, JRC, верзија 1.0, месец година
9. Техничко упутство BSI TR-03111, Криптографија елиптичних крива, верзија 2.00, 28.06.2012.
10. ISO/IEC 18033-2, Информационе технологије – Технике безбедности – Алгоритми за шифровање – Део 2: Асиметричне шифре, прво издање, 01.05.2006.
11. ISO/IEC 15408-1, -2 и -3, Информациона технологија — Технике безбедности — Критеријуми за процену ИТ безбедности, 1, 2. и 3. део, треће издање, 2008-2014.
12. ISO/IEC 8825-1, Информациона технологија - правила кодирања ASN.1: Спецификација основних правила кодирања (BER), Канонска правила кодирања (CER) и Посебна правила кодирања (DER). Четврто издање, 15.12.2008.
13. CEN EN 419 221-5 Заштитни профили за криптографске модуле TSP - Део 5: Криптографски модул за услуге од поверења
14. ISO/IEC 19790, Информациона технологија — Технике безбедности — Безбедносни захтеви за криптографске модуле, друго издање, 15.08.2012.
15. Национални институт за стандарде и технологију (NIST), FIPS PUB 140-2, Безбедносни захтеви за криптографске модуле, 25. мај 2001.

16. Национални институт за стандарде и технологију (NIST), FIPS PUB 186-4: Стандард за дигитални потпис (DSS), јул 2013.

17. ISO/IEC 9797-1, Информациона технологија – Технике безбедности – Кодови за аутентификацију порука (MAC) – Део 1: Механизми који користе блок шифре. Четврто издање, 01.03.2011.

18. Национални институт за стандарде и технологију (NIST), Посебна публикација 800-38B: Препорука за начин рада са блок шифрама: Начин рада CMAC за проверу аутентичности, 2005.

19. ISO/IEC 27001, Информациона технологија — Технике безбедности — Системи управљања безбедношћу информација — захтеви. Четврто издање, 01.10.2013.

20. Спроведбена правила за Одлуку Комисије C(2006) 3602 од 16.8.2006. године о безбедности информационих система које користи Европска комисија, усвојена 29.05.2009.

21. Одлука Комисије 2017/46 од 10. јануара 2017. године о безбедности комуникационих и информационих система у Европској комисији

22. Паметни тахограф – европска политика коренских сертификата и политика симетричних кључева инфраструктуре верзија 1.0, јун 2018.

23. Спроведбена уредба Комисије (ЕУ) 2018/5002

24. Уредба (ЕУ) 2016/679 (Општа уредба о заштити података – СЛ L 119, 04.05.2016; испр. СЛ L 127, 23.5.2018

25. Закон о радном времену посаде возила у друмском превозу и тахографима, Службени гласник РС, бр. 96/15 и 95/18;

26. Закон о заштити података о личности, Службени гласник РС, бр. 87/18

27. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Службени гласник РС, бр. 94/17

28. Закон о електронској трговини,Службени гласник РС, бр. 41/09, 95/13 и 52/19