Human Environment and Transport Inspectorate
Ministry of Infrastructure and Water Management

Issuing policy On-board computer cards and System cards, Certification Practice Statement (CPS)

Trust Service Provider IenW

On-Board Computer Taxi (BCT)

Datum	July 13th, 2020
Status	Final
Versie	4.8.2 G3 EN

Table of Content

List of Tables

List of Figures

1 Introduction

A Certification Practice Statement (CPS) is a written set of rules that describes the procedures and measures taken by a certificate service provider or Trust Service Provider (TSP) for all aspects of the Public Key Infrastructure (PKI) service. The CPS thus describes how the TSP meets the requirements stated in the applicable Certificate Policy (CP).

This document contains the English translation of the CPS that will be used to issue cards and certificates for use in the On-Board Taxi Computer (BCT). The CPS BCT was written and is managed by the TSP of the Ministry of Infrastructure and Water Management, further referred to in this document as 'IenW TSP'.

The function of the IenW TSP is to provide and manage Certificates and cryptographic keys, including the provided carrier (QSCD). The IenW TSP also has ultimate responsibility for providing the Trust Services, regardless of whether it performs the actual work itself or outsources it to others. The procedures followed and measures taken by the IenW TSP with regard to all aspects of the Public Key Infrastructure (PKI) are described in this document. The activities and responsibilities of the IenW TSP apply to the issuance of cards and Certificates for use in the Onboard Computer Taxi (BCT).

In case of ambiguity of this translation the explanation and interpretation of the Dutch version will be leading and decisive.

1.1 Overview~~Background~~

1.1.1 On-Board Taxi Computer

In its position paper on "Taxi to the Future", the Dutch government is pursuing a policy for a better taxi product at a fair price. The government has initiated various steps for this purpose. For example, there are stricter quality requirements for licences for taxi businesses and drivers, intensification of supervision, the introduction of a transparent tariff structure and introduction of an On-Board Taxi Computer. The on-board computer will provide electronic registration of the legal obligation to record the taxi journeys performed and the working, driving and rest times of the drivers.

The BCT has the following required main functionalities, laid down in the ministerial order for "Specifications and type approval of On-Board Taxi Computer":

- Digital recording of the journey records;
- Digital recording of working and rest times;
- Possibility to connect operating equipment;
- Provision of data available for the purpose of a receipt;
- Automatic position-fixing of the start and end locations of journeys.

The BCT uses electronic signatures to guarantee the integrity of the data.

1.1.2 *Types of cards and certificates*

There are in total of six different types of cards linked to the use of the BCT. All of these cards contain a chip on which one or more certificates and associated key pairs are stored.

Five of the card types are used to identify the users of the BCT. These cards are called on-board computer cards (BCT cards). The last type of card gives the on-board computer system its identity. This is the system card.

A distinction is made between the following cards:

- **Driver card**
  Identifies the driver and records his/her activities. This card contains one personal signature certificate and one personal authentication certificate.

- **On-the-job training card**
  Gives the driver the option of using the on-the-job training scheme ('LWT') for taxi drivers. This allows him/her (for a period not exceeding four months) to perform certain kinds of taxi transport without holding a tax driver's diploma. Its working is exactly the same as the Driver card, except that its validity is 4 months. Therefore, this card is not specified any further in this CPS.

- **Business card**
  Identifies the taxi business and unlocks access to the data stored for this business in the BCT. This card contains one non-personal service certificate for authentication.

- **Control card**
  Identifies the accredited workshop and unlocks access to the on-board computer for testing and calibration. This card contains one non-personal service certificate for authentication.

- **Inspection card**
  Identifies the supervisor and unlocks access to the data stored in the on-board computer's memory for reading and/or transfer. This card contains one personal authentication certificate and one personal signature certificate.

- **System card**
  Identifies the on-board computer and enables it to sign data. This card contains one non-personal service certificate for authentication.

All certificates on the cards are of the X509v3 type.

The term of validity of the personal BCT cards (Driver and Inspection cards) and BCT services cards (Business and Control cards) is five years.
The System card is valid for a minimum of 5 years and a maximum of 10 years. The actual term of validity is limited by the expiration date of the CA hierarchy.

In all instances the validity term of the certificates on the cards is limited by the expiration date of the CA hierarchy. For the G3 this is 14 November 2028 for the Root CA certificate. This means that an end-user certificate will be valid up to and including 11 November 2028.

The on-the-job training card is valid for four months, followed by a BCT Driver card valid for 5 years.

The BCT cards have dedicated features and different procedures for application and delivery.

1.1.3 *CA hierarchy*

The Ministry of Infrastructure and Water Management creates its Public Key Infrastructure (PKI) under the trust structure of the PKI of the State of the Netherlands ('PKIoverheid') and has thus opted for the root certificate of the "State of the Netherlands" as the highest trust point. For this purpose, the Ministry has set up a Trust Service Provider (TSP) that is part of PKIoverheid, the so-called IenW TSP.

The BCT cards and System cards will be issued by Kiwa Register BV (KIWA) under the responsibility of the IenW TSP. Under a mandate of the Minister of Infrastructure and Water Management, KIWA will issue licences for various modalities, including BCT cards.

1.1.4 *PKIoverheid*

PKIoverheid facilitates the Public Key Infrastructure for the Dutch authorities. To this end, PKIoverheid manages the root certificate of the State of the Netherlands. This Root Certificate Authority (CA) is the highest (self-signed) CA and is owned by the State of the Netherlands.

Under this Root CA, various domain CAs have been issued. These domain CAs are signed by the Root CA and in turn the TSP CAs sign. The TSP CAs sign the certificates for users and systems.

The following figure shows the domains for which the TSP of the Ministry of Infrastructure and Water Management issues certificates under the G3 Root CA. For the sake of completeness, the various types of end-user certificates have also been included:

- A: Personal certificate for authentication
- Esig: Personal certificate for electronic signature
- SA: Organisational services certificate for authentication
- AA: (Autonomous) device-specific certificate for authentication

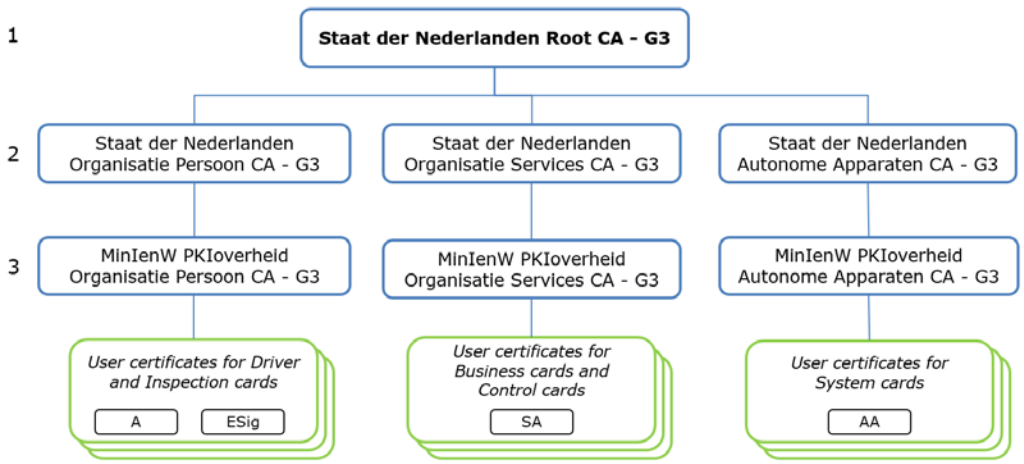

Figure 1 – PKIoverheid hierarchy G3

The hierarchy of PKIoverheid is described in the Statement of Requirements (SoR) of PKIoverheid (Part 1, Introduction SoR). The Root CA (level 1) and the domain CAs (level 2) are managed by PKIoverheid. The TSP CAs (level 3) are issued by PKIoverheid but are managed by the TSP.
A description of the management of these CAs can be found in the CPS Policy Authority PKIoverheid for certificates issued by the Policy Authority of PKIoverheid. These documents can be found at https://www.logius.nl/diensten/pkioverheid.

1.2 Document Name and Identification ~~CPS purpose and references~~

The CPS of the IenW TSP describes how the PKI services for the BCT are implemented. The CPS describes the processes, procedures and controls for applying for, producing, providing, managing and revoking the BCT and System card certificates. By means of the CPS, those involved can determine their confidence in the services provided by the IenW TSP. The general structure of this CPS follows the model presented in the *Request for Comments (RFC) 3647*.

Formally, the present document is referred to as the "Issuing Policy for On-Board Computer Cards and System Card, Certification Practice Statement", or CPS for short.

1.3 PKI Participants ~~Parties involved~~

~~The following parties are involved in the issue of cards:~~
IenW TSP (vested in the Rail and Road transport domain of the Human Environment and Transport Inspectorate, which is part of the Ministry of Infrastructure and Water Management), ~~including~~ is responsible for issuing cards, involving the following suppliers of services and products:
- Card issuer (Kiwa Register B.V.)
- Personaliser (IDEMIA The Netherlands B.V.)
- Certificate producer (KPN B.V.)
- Distributor (AMP Logistics B.V.)

The following PKI end-users (roles) relating to the use of certificates are identified:
- Subscribers
- Certificate holders
- Certificate administrators
- Relying parties

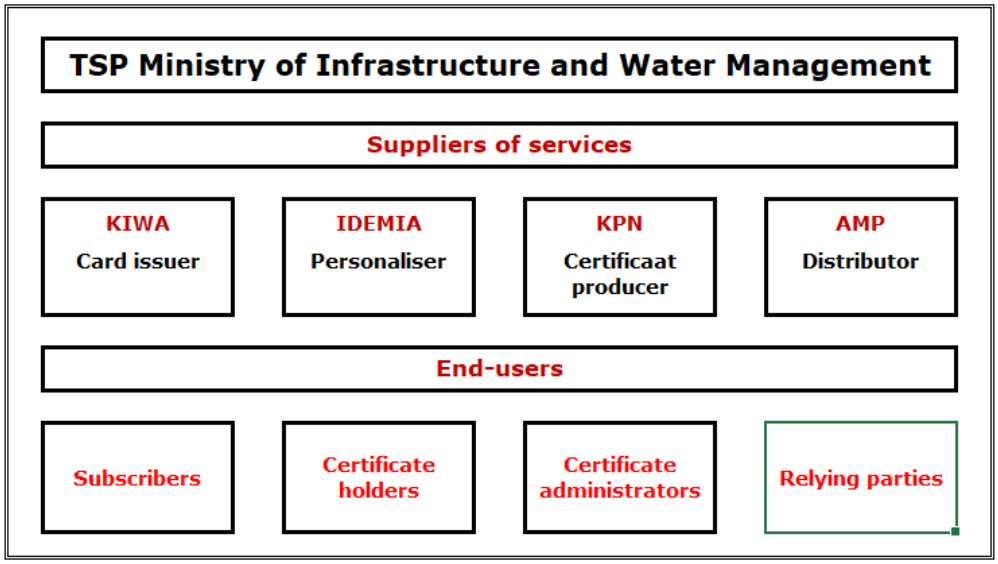

Figure 2 – PKI Participants ~~Parties involved~~

1.3.1 *Trust Service Provider Ministry of Infrastructure and Water Management (TSP)*

The TSP CA certificates of the Ministry of Infrastructure and Water Management are the starting point for trust within the hierarchy of the PKI of the ministry. This determines the trust placed in all end-user certificates issued under the responsibility of the Ministry of Infrastructure and Water Management.

The TSP fulfils the role of PKIoverheid TSP and is ultimately responsible for rendering all certification services provided on behalf of the Ministry of Infrastructure and Water Management.

For there to be a reliable PKI hierarchy, it is important for the TSP management function to work reliably. This management function guarantees the reliability of the TSP CA certificates by applying adequate security measures.

The TSP will demonstrate reliable working by submitting to the regular supervision by the Policy Authority (PA) of PKIoverheid.

The PA will require the TSP to conform to the PA's regular supervisory process, as is the case for every TSP that has joined the PKIoverheid hierarchy.

In this system, an annual conformity assessment takes place at the TSP and delegated third parties.

With the implementation of the eIDAS Regulation (Electronic Identification and Trust Services for Electronic Transactions in the Internal Market), the new Telecommunications Act and the NetSec requirements from the CAB forum, the audit cycle will be carried out according to the ETSI EN 319 403 certification model. The IenW TSP will undergo a certification audit once every 2 years. A full audit will be conducted annually in the intervening year.

1.3.2 Card issuer

The card issuer will take care of the processing of certificate applications and all related tasks. The card issuer physically collects the identification data, checks and records it and performs the described verification checks.

The card issuer will use multi-factor authentication for the system or all user accounts usable to issue or approve certificates.

However, the card issuer will have implemented technical measures, so that a user account can validate certificate applications only based on a pre-approved list of domains or e-mail addresses.
After the checks, the card issuer will instruct the personaliser to produce the BCT cards, and the certificate producer to produce certificates. After the cards have been produced, they will be issued by the distributor to the certificate holders.

Requests for revoking a certificate will be addressed to the card issuer. The card issuer will check whether the request meets the applicable conditions and, subject to a positive assessment, will instruct the certificate producer to revoke the relevant certificate.

1.3.3 Personaliser

The BCT cards will be graphically personalised by the personaliser based on production orders from the card issuer. The production orders will further serve as a basis for generating the key material and certificate applications that will be sent by the personaliser to the Certificate producer. The resulting certificates will then be placed on the BCT cards and sent to the distributor.

1.3.4 Certificate producer

The certificate producer will take care of the production of requested certificates based on an authenticated request from the personaliser. The certificates are sent to the personaliser immediately after they have been created.

The certificate producer will publish revoked certificates in the Certificate Revocation List (CRL). Revoked certificates will be published in a CRL only after the certificate producer has received from the card issuer a message to revoke the certificate.

1.3.5 Distributor

The distributor will physically issue the cards supplied by the personaliser, including the activation data to the certificate holder and/or certificate administrator.

1.3.6 Subscriber, Certificate Holder and Certificate Administrator.

The subscriber will be the party that enters into an agreement with the TSP for supplying certificates to the subscriber. Thereby, the subscriber will represent the certificate holder.

The certificate holder will be identified in the certificate as the holder of the private key that corresponds with the public key included in the certificate.

A certificate administrator will be authorised to perform actions on behalf of the subscriber and in relation to the certificate holder which the certificate holder personally is unable to do.

Table 1 shows the relationship between the subscriber and the certificate holder for each card type.

Card type	Subscriber	Certificate holder
Driver card	Taxi driver	Taxi driver
Inspection card	Inspection department/test department	Inspector/controller
Business card	Taxi business	Taxi business
Control card	Accredited workshop	Accredited workshop
System card	On-board computer manufacturer	On-board computer

Table 1 – Relationship Subscriber – Certificate Holder

1.3.7 Relying parties

A trusting party is the party in trust that acts on a certificate. The category of relying parties in this case consists of anyone who acts in trust on BCT certificates, with the possible objectives of authenticating cardholders, verifying an electronic signature or encrypting communication with that party.

1.4 ~~Use of C~~ertificate Usage

The scope of the personal certificates issued by the IenW TSP will be limited to the user community consisting of the subscribers, certificate holders and relying parties referred to in paragraph 1.3 of Part 3a of the SoR PKIoverheid.

Personal certificates will be subdivided into professional and organisational certificates.

Professional certificates will be for use by natural persons who use the certificate for their work.

Organisational certificates will be issued to natural persons who use the certificate on behalf of the subscriber, including inspectors of the Human Environment and Transport Inspectorate and employees of other inspectorates.

In addition to the personal certificates, non-personal certificates will be used by test bodies and taxi businesses. These services certificates are described in paragraph 1.4, Part 3b of the SoR PKIoverheid.

The System card used in the BCT will contain an "Autonomous Device Certificate". The use of this certificate is described in paragraph 1.4, Part 3d of the SoR PKIoverheid.

Additionally, there will be relying parties that act in trust on certificates from the relevant certificate holders. A trusting party is any natural or legal person who is a recipient of a certificate and acts in trust on that certificate. The applicability of the certificates is further explained in Table 2:

Type	Usage
Personalised Authentication certificate	This certificate will be used to authenticate the certificate holder
Personalised Signature certificate	This certificate will be used to verify an electronic signature
Services certificate (authentication)	This certificate will be used to authenticate the certificate holder
Autonomous device certificate (authentication)	This certificate will be used for authentication of the BCT.

Table 2 – Scope of application

Certificates may be used only for the stated purpose (for use in the BCT). There are no technical limitations to the use of the certificates.

The BCT Driver card is not a recognised means of identity and therefore cannot be used as such.

1.5 Policy Administration ~~CPS management~~

1.5.1 *Contact details*

Information about this CPS or the services of the IenW TSP can be obtained using the contact details below. Comments on the underlying CPS may be sent to the same address.

Human Environment and Transport Inspectorate
For the attention of Trust Service Provider IenW
PO box 20901
NL-2500 EX The Hague

dci.csp@minienw.nl

More information about the services of the TSP of the Ministry of Infrastructure and Water Management is obtainable via https://bct.tsp.minienw.nl

1.5.2 *Change and approval of CPS*

The IenW TSP will have the right to change or supplement the CPS. Changes will apply from the moment the new CPS is published. The procedure for changing and approving the CPS is described in paragraph 9.11.

1.6 Definitions and Acronyms ~~abbreviations~~

An overview of the definitions and abbreviations used in this document is provided in Annex A and Annex B.

2 Publication and Repository Responsabilitiesy ~~for publication and electronic storage~~

2.1 Electronic storage

The electronic storage location of the IenW TSP is publicly accessible via https://bct.tsp.minienw.nl/

2.2 Publication of TSP information

The IenW TSP will publish the following TSP information:

- Certification Practice Statement (CPS)
- Terms and conditions
- PKI Disclosure Statement (PDS)
- Certificates Revocation Lists (CRLs)
- CA certificates

The table below shows where the data will be made available:

Type of information	URL
CPS	https://bct.tsp.minienw.nl/minienw-bct-cps
Terms and conditions	https://bct.tsp.minienw.nl/minienw-bct-av/minienw-bct-av.pdf
CRL Driver and Inspection cards	https://bct.tsp.minienw.nl/minienw-org-pers-ca-g3.crl
CRL Business and Control cards	https://bct.tsp.minienw.nl/minienw-org-serv-ca-g3.crl
CRL System cards	https://bct.tsp.minienw.nl/minienw-aa-ca-g3.crl
CA Driver and Inspection cards	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer
CA Business and Control cards	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer
System cards CA	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer

Table 3 – URLs G3

The laws and regulations referred to in this CPS can be consulted on the website https://wetten.overheid.nl

For the Certificate Policies (CP), reference is made to https://www.pkioverheid.nl/. In order to identify the correct CP, the following table shows the relationship between the cards, the functions of the certificates, the applicable CP and the Object Identifier (OID) of the CP.

Type of certificate – Card type	Policy identifiers (OID)	CP
Personal authentication certificates: Driver card Inspection card	2.16.528.1.1003.1.2.5.1	OID of the PKIoverheid Certificate Policy for personal authentication certificates in the Organisation domain.
Personal signature certificates: Driver card Inspection card	2.16.528.1.1003.1.2.5.2	OID of the PKIoverheid Certificate Policy for personal signature certificates in the Organisation domain.

Type of certificate – Card type	Policy identifiers (OID)	CP
Services authentication certificates Control card Business card	2.16.528.1.1003.1.2.5.4	OID of the PKIoverheid Certificate Policy for services certificates for authentication in the Organisation domain
Autonomous device certificate: System card	2.16.528.1.1003.1.2.6.1	OID of the PKIoverheid Certificate Policy for Device-bound authentication in the Autonomous Devices domain.

Table 4 - Card type and applicable Certificate Policy (CP)

2.3 Time or frequency of publication

The publication of Certificates Revocation Lists (CRLs) takes place every three hours. In the event of a change, the other information referred to under 2.2 will be updated as quickly as necessary.

2.4 Access to published information

The published information stated in 2.2. is in the public domain and freely accessible. The published information can be consulted electronically twenty-four hours a day and seven days a week, with the exception of system defects and maintenance work.

If the electronic storage location is unavailable, availability will be restored within 24 hours.

3 Identification and Authentication (I&A)

3.1 Naming

This section describes how the identification and authentication of applicants will take place during the initial registration procedure and the criteria the IenW TSP sets with regard to names.

3.1.1 *Types of name formats*

All certificates issued by the IenW TSP will contain information about the organisation of the applicant. For Driver cards and Inspection cards, personal name details will also be included in the certificate.

The names in the certificates will be structured as described in the following table:

Attribute (X.500)	Driver card	Business card	Control card	Inspection card	System card
issuer.countryName	NL	NL	NL	NL	NL
issuer. organisationName	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat
issuer. organisationIdentifier	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179
issuer. CommonName	MinIenW PKIoverheid Organisatie Persoon CA - G3	MinIenW PKIoverheid Organisatie Services CA - G3	MinIenW PKIoverheid Organisatie Services CA - G3	MinIenW PKIoverheid Organisatie Persoon CA - G3	MinIenW PKIoverheid Autonome Apparaten CA - G3
Subject.CountryName	NL	NL	NL	NL	NL
subject.organisationName	[First name] [Additional initials] [Prefix] [Family name]	[Business name]	[Name of test body]	[Name of inspection authority]	[On-board computer manufacturer name]
Subject. organisationIdentifier	n/a	NTRNL- [Chamber of Commerce number of business]	NTRNL- [Chamber of Commerce number of test authority]	n/a	n/a
Subject. CommonName	[First name] [Additional initials] [Prefix] [Family name]	[Business name]	[Test body name]	[First name] [Additional initials] [Prefix] [Family name]	[Type approval number]
Subject.givenName	[First name] [Additional initials]	n/a	n/a	[First name] [Additional initials]	n/a
Subject.surName	[Prefix] [Family name]	n/a	n/a	[Prefix] [Family name]	n/a
Subject. SerialNumber	[Card Main Type] + [CSN] + "-" + [Card Serial Number] or Card Main Type + [NR Number] + "-" [Card Serial Number]	[Card main type] + [Chamber of Commerce number] + "-"+ [Card serial number]	[Card Main Type] + [RDW approval number] + "-" + [Card serial number]	[Card Main Type] + [Inspection Number] + "-" + [Card Serial number]	[Card Main Type] + [On-board Computer Number] + "-" + [Card Serial number]
Subject.Title	CVOL or CBEP	O	K	I	S
subjectAltName.otherName PermanentIdentifier. identifierValue	[Card Main Type] + [CSN] or [Card Main Type] + [NR-Number]	[Card Main Type] + [Chamber of Commerce number]	[Card Main Type] + [RDW approval number]	[Card Main Type] + [Inspection number]	[Card Main Type] + [On-board computer number]
PermanentIdentifier. assigner	2.16.528.1.1003.1.3.10.1.1	2.16.528.1.1003.1.3.11.1.1	2.16.528.1.1003.1.3.11.1.1	2.16.528.1.1003.1.3.10.1.1	2.16.528.1.1003.1.3.6.2.1
certificatePolicies. PolicyIdentifier	2.16.528.1.1003.1.2.5.1 (Aut) 2.16.528.1.1003.1.2.5.2 (ESig)	2.16.528.1.1003.1.2.5.4	2.16.528.1.1003.1.2.5.4	2.16.528.1.1003.1.2.5.1 2.16.528.1.1003.1.2.5.2	2.16.528.1.1003.1.2.6.1

Table 5 - Data in certificates

The data supplied by the applicant will be verified using reliable sources. The supplied data will consist of characters from the Municipal Database (GBA) character set, coded as UTF8.

In case of long names it may happen that the IenW TSP is forced to apply shortening rules for the commonName, givenName and surName. These shortening

rules are specified in detail in the “MinIenW TSP PKIoverheid Certificate Profiles BCT G3”.

Unique OID numbers (Object Identifiers) will be assigned to the TSP within PKIoverheid. This number will be used in different fields of the different certificates.

The following OIDs have been assigned by the Policy Authority of PKIoverheid to the Ministry of Infrastructure and Water Management. The OIDs have been issued for the organisation of the Ministry of Infrastructure and Water Management and for the underlying CA Certificates issued for the IenW TSP.

OID	Meaning
2.16.528.1.1003.1.3.10.1	minienw (PKIO domain organisation person)
2.16.528.1.1003.1.3.10.1.1	minienw.organisation-person-tsp.ca
2.16.528.1.1003.1.3.11.1	minienw (PKIO domain organisation services)
2.16.528.1.1003.1.3.11.1.1	minienw.organisation-services-tsp.ca
2.16.528.1.1003.1.3.6.2	minienw (PKIO domain autonomous devices)
2.16.528.1.1003.1.3.6.2.1	minienw.autonomous-devices-tsp.ca

Table 6 - OIDs issued by PKIoverheid to the Ministry

Field definition

a) Cardholder number

The following table shows the lengths and types of fields used in the certificates of all card types:

Card type	Field content	Type and length
Driver card	CSN or NR number of the driver	Text 9
Business card	Chamber of Commerce number	Text 12
Control card	RDW approval number	Text 7
Inspection card	Inspection number	Text 10
System card	A unique on-board computer number generated by the IenW TSP	Text 9

Table 7 - Cardholder number field content

For the Driver card, the Citizen Service Number (CSN) will be used for persons who have a CSN. For persons who do not have a CSN, a Non-Resident Number (NR number) will be generated.

b) Card type

The card types used by the IenW TSP are:
- **D**river card
- **B**usiness card
- **C**ontrol card
- **I**nspection card
- **S**ystem card

Different card types are possible for the cards.

Card type	User group	Content
Driver card	Driver	CVOL or CBEP
Business card	Carrier	O
Control card	Workspace	K
Inspection card	Supervisor	I
System card	On-board computer	S

Table 8 – Card type

The card type will be used within the BCT to determine access privileges and operating mode.

c) Card serial number

This number will be used to uniquely identify the card within the combination of cardholder number and card type. This will be used for the existence of several cards per cardholder at the same moment in time (for the Business card and the Control card) and for the replacement of cards. This field is 5 characters long and of the text type.

Card serial numbers will start with 00001 and increase sequentially.

3.1.2 Need for meaningful name

Names used in the issued certificates will be such as to enable the trusting party to establish irrefutably the identity of the certificate holder or subscriber.

3.1.3 Anonymity pseudonym and wildcards in certificates

The IenW TSP does not allow the use of pseudonyms and wildcards.

3.1.4 Guidelines for interpreting the various name forms

The following points are relevant to the interpretation of the name:

1. The commonName in certificates on the Driver card and Inspection card will contain the family name of the holder including prefixes and first names, as stated in the identification document submitted at registration. Acceptable identification documents will be the valid documents referred to in Section 1 of the Compulsory Identification Act.

2. In the commonName mentioned in item 1, only the first name will be stated in full, while the other names will be abbreviated in accordance with the identification document submitted at registration. If the resulting commonName contains more characters than is technically possible, one or more initials will be omitted, starting with the last initial, until the created commonName does fit.

3. The commonName in certificates on the Business card and Control card will contain the organisation name as it appears on the document for identification of the organisation submitted at registration.

4. The commonName in the certificate on the System card contains the type approval number issued by RDW for the relevant type of on-board computer.

5. The organisationName in the certificates of all card types will correspond with the organisation name referred to in item 3, with the exception of the Driver card where the organisationName and commonName will be the same.

The IenW TSP reserves the right to alter the requested name at registration if this is legally or technically necessary.

3.1.5 *Uniqueness of names*
The IenW TSP will guarantee that the uniqueness of the "subject" field is assured. This means that the distinctive name used in an issued certificate can never be assigned to another subject. This will be accomplished by means of the card type, cardholder number and card serial number stated in the subject.serialNumber field.

3.1.6 *Recognition, authentication and the role of trademarks*
The name of an organisational association as registered in the Chamber of Commerce Trade register, will be used during registration and in the certificates. The subscribers bear full responsibility for any legal consequences of using the name they provide. In the event that brand names are used, the IenW TSP will take the necessary care, but is not obliged to initiate an investigation into possible violations of trademarks as a consequence of using a name which is part of the details included in the certificate. The IenW TSP reserves the right to change the requested name if it could be contrary to trademark law.

3.2 Initial Identity Validation

3.2.1 *Proof of possession of "private key associated with the certificate to be issued"*
The IenW TSP does not provide certificates for key pairs not generated by the IenW TSP itself. The key pairs will be generated by the personaliser in a controlled and protected area as part of the personalisation procedure in a secure cryptographic module. The certificate applications will then be sent to the certificate producer using a secure communication protocol. After the processing and return of the certificates, the certificates and private keys will be injected into the card using a secure communication session. The private key cannot leave the card.

3.2.2 *Authentication of organisational identity*
During the application for a card, the subscriber will submit data showing the identity of the organisation to be included in the certificates. The exception to this is the Driver card. In this card, the identity of the cardholder will be the same as the organisational identity.

The following data, and the associated evidence, will be supplied and recorded during the application process:

Data	Card type
Chamber of Commerce number	Control card, Business card, System card
Taxi licence number	Business card
RDW approval number	Control card
Human Environment and Transport Inspectorate number	Inspection card
Type approval number	System card

Table 9 - Application data of organisational entity

Based on the supplied data, the IenW TSP will use reliable registers to determine whether the organisation exists and is authorised to make an application. The information about the organisation to be included in the certificate, such as the organisation name, will be copied from the reliable registers.

3.2.3 Authentication of personal identity

Certificate holder and certificate administrator will be distinguishable when establishing a personal identity. The personal identity of the certificate holder will be established in the case of the Driver card and Inspection card. For the business, test, inspection and System cards, this check will concern the certificate administrator.

During the application for a card, the following information about the certificate holder will be supplied by the subscriber:

Data	Card type
CSN	Driver card, Inspection card
Date of birth	Driver card, Inspection card
Human Environment and Transport Inspectorate number	Inspection card
Inspection number (Special Investigator)	Inspection card

Table 10 – Application data of certificate holder

If a prospective certificate holder does not have a CSN, the subscriber will supply the data applicable to the certificate administrator during the application for a card.

A subscriber will supply the following information about the certificate administrator and the associated proof:

Data	Card type
Full name, including surname, first name, initials or other first name(s) (if applicable) and middle names (if applicable);	Driver card, Inspection card, Business card, Control card, System card
Date and place of birth, a nationally appropriate registration number, or other characteristics of the certificate holder or administrator that can be used to distinguish, as far as possible, this person from other persons with the same name	Driver card*, Inspection card, Business card, Control card, System card

Data	Card type
Proof that the certificate administrator is entitled to receive a certificate for a certificate holder on behalf of the legal person or other organisational entity	Inspection card, Business card, Control card, System card

Table 11 - Application data of certificate administrator

In the case of the Driver card and Inspection card, the distributor will validate the identity of the certificate holder on the basis of a personal check on the certificate holder in combination with an identity document referred to in Section 1 of the Compulsory Identification Act.
In the case of the Business card, Control card and System card, the identity of the certificate administrator will be validated on the basis of the proof submitted with the application.

This validation will occur at the time and place agreed with the distributor by the certificate holder/certificate administrator.

3.2.4 *Unverified data*

The IenW TSP will verify the name of the subscriber based on acceptable documents and reliable registers. All application data included in the certificate will also be verified.

Data recorded for correspondence purposes only, such as a postal address and telephone numbers, will not be verified. Data not verified will be taken by the IenW TSP from the application form signed by an authorised applicant on behalf of the subscriber.

3.2.5 *Certificate holder authorisations*

During an application for a BCT card, the IenW TSP will determine whether an applicant is authorised to submit the application on behalf of the subscriber.

3.2.6 *Requests for cross-certification and other forms of interoperation*

Not applicable. The BCT does not use cross-certification or other forms of interoperation.

3.3 I&A for Re-key requests ~~Identification and authentication when renewing the certificate~~

3.3.1 *Routine renewal of the certificate*

Routine certificate renewal will not be offered by the IenW TSP. If a BCT card is about to expire, the certificate holder or certificate administrator will have to re-apply for a card.

3.4 I&A for Revocation Requests ~~Identification and authentication for revocation requests~~

Requests for revocation of certificates will be linked to the revocation procedure of the BCT cards.

An electronic request for revocation of a BCT card will be checked for authenticity using the revocation code. This code will be provided to the certificate holder or

certificate administrator as part of the issuing process. The code is uniquely linked to the BCT card.

Holders of a Driver card will have the option of requesting a replacement card. Before a replacement Driver card is issued, the certificates of the old card will be revoked. The certificate holder will not have to submit a separate request for this.

In the case of a revocation request by telephone, the submitter must answer a number of pre-determined questions. This enables the IenW TSP to obtain sufficient certainty about the identity of the requester of the revocation and the on-board computer card for which revocation is requested.

4 ~~Operational Requirements for the~~Certificate Life-Cycle and Operational Requirements

4.1 ~~Application for C~~ertificate Application

Applications for certificates will form part of the application for a card. These applications may be submitted only by subscribers.

4.1.1 *Subscriber registration process*

The registration process for a subscriber will have two variants, depending on the type of card requested.

For the card types of Driver card, Business card and Control card, the registration of the subscriber will form part of the card application process.

The registration of the subscriber will not form part of the application process for the Inspection card and the System card. For these two card types, the subscriber must register with the IenW TSP before applying for the card. For this purpose, the appropriate form must be completed, signed and submitted with the necessary supporting documents in writing to the IenW TSP.

The subscriber registration must in all cases be performed by the authorised representative of the subscriber. For applications for the System card and on-board computer cards other than the Driver card, a certificate administrator may be designated by the authorised representative.

By submitting a registration application, the prospective subscriber will accept the contents of this CPS and the terms and conditions. The subscriber is held to regulations for the use of the on-board computer and on-board computer cards.

4.1.2 *Process of applying for cards*

An application for a Driver card, Business card or Control card must be submitted by the prospective subscriber. For this purpose, the appropriate application form must be completed, signed and submitted with the required supporting documents in writing to the IenW TSP.

The contact person designated by the subscriber may submit an application for an Inspection card by e-mail to **NL.Wegvervoer@kiwa.nl** ~~**vergunningen@kiwa.nl**~~

The e-mail must contain the following information about the relevant certificate holder:

- Full name (first names in full)
- Date of birth
- Special Investigator record number
- The inspection number of the subscriber

The card issuer will send the subscriber by post an application set for each requested Inspection card. The application set will consist of:

- Accompanying letter
- Application form (in the name of the relevant certificate holder) with space for passport photo

- Explanatory notes to the application
- return envelope

The contact person of the subscriber must ensure that the relevant certificate holder receives the application form, places his/ her photo according to the provided instructions, signs the form and returns it to KIWA within 4 weeks.

The payment owed for the Inspection card is payable by means of the concluded "pay later" agreement.

The card issuer will process the application as soon as is receives the application set. The Inspection card will be produced after approval of the application.

When delivering the Inspection card, AMP will check the identity of the certificate holder.

When applying for a System card, the certificate administrator will state only how many System cards are required. The other data will be taken from the subscriber registration.

By submitting a card application, the prospective certificate holder/certificate administrator will accept the contents of this CPS and the terms and conditions. The certificate holder/certificate administrator is held to regulations for the use of the on-board computer and on-board computer cards.

4.1.3 *Renewal of cards on the initiative of TSP and card issuer*

If there is a technical need, the TSP may decide to renew cards and "push" them to the certificate holders. The card issuer will rely on the data already received and, on that basis, will produce a card with start date validity related to production date and end date validity equal to the card to be replaced. Issuance including determination of identity will take place in accordance with the regular process.

4.2 ~~Processing of~~Certificate application Processing

The card issuer will receive the card application and will assess the completeness and accuracy of the application. During this assessment, the identity of the applicant will be determined in accordance with paragraph 3.2 of this CPS. If the applicant meets the prescribed requirements, the card application will be approved.

4.3 Certificate Issuance

After approval of the card application, the card issuer will place a production order for the card with the personaliser.

Based on the production order, the personaliser will create a key pair for the card. The personaliser will then submit a certificate request to the certificate producer using the data from the production order and the created public key of the key pair.

The certificate producer will subsequently issue a certificate in accordance with the certificate request and will return the result to the personaliser and to the card issuer.

The personaliser will receive the certificate and place it on a card with the corresponding private key. To this end, activation data will be created for the card. The card will then be graphically personalised using the data from the production order.

After production of all types of BCT cards, they will be entrusted to the distributor for safekeeping. The certificate holder or subscriber will receive a positive decision with:

- The user instruction for revocation;
- The delivery message with the possibility to make arrangements with the distributor for the time and place of desired delivery via **https://www.mijnafspraak.nl/**

The Business card, Control card and System card will be received by a designated employee of the subscriber, who is authorised to perform the role of certificate manager on behalf of the subscriber for relevant cards and certificates. The name of the employee is being recorded by the distributor.

Before handing over the card, the Distributor checks the correctness of the data on the card. Before taking possession of the card, the recipient will be able to check correctness of the data on the card. If the data are incorrect, the distributor must take these cards back with him, report this immediately to the card Issuer and deliver them to the card Issuer.

In all cases, a signature must be provided for receipt of the card, indicating that the certificate holder/certificate administrator accepts the contents of this CPS, the terms and conditions and the correctness of the data on the card, insofar as this has not already occurred.

The activation data will in all cases be sent by the personaliser directly to the certificate holder/certificate administrator.

4.4 ~~Acceptance of~~ Certificate~~s~~ Acceptance

4.4.1 *Acceptance by certificate holder / certificate administrator*
Acceptance of certificates will be deemed to have occurred after the transfer of the on-board computer card to the certificate holder/certificate administrator.

4.4.2 *Publishing of end-user certificates*
The IenW TSP will not publish end-user certificates. C~~A c~~ertificates will be ~~published~~ distributed as part of the process of issuing the~~se certificates~~ on-board computer cards and system cards.

4.4.3 *Notifcation of certificate issuance to third parties*
During the production process, the certificate producer shares the certificates with the personaliser and the card issuer. No further notification of certificate issuance to third parties takes place.

4.5 Key Pair and Certificate Usage

The responsibilities and in particular the associated obligations of the subscriber, the certificate holder/certificate administrator and relying parties will be described in the set of the regulations for use of the on-board computer and on-board computer card scheme, the CPS and the terms and conditions.

4.5.1 *Subscriber responsibilities and obligations*

The subscriber will be responsible for the correct, timely and complete supply of all data necessary for creation and delivery and for correct use of the certificates. The subscriber will guarantee the IenW TSP and relying parties its correct, timely and complete compliance with the guidelines laid down in this CPS and the terms and conditions.

4.5.2 *Responsibilities and obligations certificate holder/certificate administrator*

The certificate holder/certificate administrator will act as the holder of the certificate requested for the certificate holder on behalf of the subscriber. He will further be responsible for the correct supply of all data necessary for creating and delivering certificates, as well as for the correct use of the certificates. The certificate holder will guarantee the IenW TSP and the other stakeholders his correct, timely and complete compliance with the guidelines set out in this CPS and the terms and conditions.

4.5.3 *Responsibilities and obligations of relying parties*

The trusting party will be responsible for correctly relying on a certificate and will guarantee the IenW TSP and the other stakeholders its correct, timely and complete compliance with the guidelines set out in this CPS and the terms and conditions.

The following obligations will apply to the trusting party:

- ~~Verify the validity of the certificate by means of the most recently published Certificate Revocation List (CRL);~~
- Take note of all obligations regarding the use of the certificate as stated in the present CPS and the terms and conditions, explicitly including all restrictions on the use of the certificate;
- ~~Take all other precautionary measures that may reasonably be taken by relying parties;~~
- Be aware that previous checks authenticate only the integrity of the data and the identity of the certificate holder, which explicitly does not imply an opinion on the content of the data.

4.6 Certificate Renewal

The IenW TSP will not offer any possibility to renew PKIoverheid certificates. A request for renewal will be treated as a request for a new certificate, whereby a new key pair will be generated.

4.7 Certificate Re-key ~~of certificates~~

Keys of certificate holders will not be reused after expiry of the term of validity or after revocation of the corresponding certificates.

4.8 ~~Alteration of C~~Certificates Modification

The IenW TSP will not offer any possibilities to alter the content of PKIoverheid certificates. If the data in the certificate no longer correspond with reality, the subscriber must immediately request revocation. If desired, an application may be made for a new card.

4.9 Certificate Revocation and Suspension ~~of certificates~~

4.9.1 *Circumstances leading to revocation*

In the following cases, the subscriber and/or certificate holder will be obliged immediately to submit a request for revocation of the certificate to the IenW TSP without delay:

- Loss, theft or malfunction of the on-board computer card;
- Detected or suspected misuse or compromise of the certificate;
- Definitive blocking of the on-board computer card after entering an incorrect PUK code three times;
- Inaccuracies in the content of the certificate;
- Alteration of the data stated in the certificate;
- Alteration of the data required for the reliability of the certificate;
- Death of the certificate holder (in the case of personal certificates);
- If the IenW TSP receives notification of death concerning the certificate holder of professional certificates, the IenW TSP will perform a verification in the Municipal Database. If the Municipal Database confirms the death, the IenW TSP will invoke the revocation procedure[1].
- Termination of the relationship between subscriber and certificate holder;
- Termination of the organisational unit (in the case of services certificates);
- Dissolution or bankruptcy of the legal person of the subscriber (in the case of service certificates).

If the subscriber indicates that the original request for a certificate was not permitted and the subscriber does not grant retroactive permission, the certificate will be revoked by the IenW TSP.

If the certificate holder suspects that his PIN has become known, but is also certain that the on-board computer card has not been out of his possession, the certificate holder may personally change the PIN so that the card does not have to be revoked.

Certificates may be revoked by the IenW TSP without further notice if:

- The IenW TSP has sufficient proof that the subscriber's private key has been compromised or is suspected to have been compromised, or there is an inherent security weakness, or that the certificate has been misused in some other way. A key will always be considered compromised in the event of unauthorised access or suspected unauthorised access to the private key, or in the event of a lost or presumably lost private key or QSCD, or stolen or presumably stolen key or QSCD or destroyed key or QSCD;
- If the subscriber, the certificate holder and/or the certificate administrator fails to meet the obligations contained in this CPS, the regulations for use of the on-

[1]Three months before a Driver card renewal, the IenW TSP will verify the owner of a Driver card in the Municipal Database. If the Municipal Database provides feedback that the person has died, no request for renewal will be sent.

board computer and on-board computer cards, the terms and conditions or the agreement concluded with the subscriber;
- The IenW TSP is informed or otherwise becomes aware of a substantial change in the information contained in the certificate;
- The IenW TSP determines that the certificate was not issued in accordance with this CPS, the regulations for use of the on-board computer and on-board computer cards, the terms and conditions or the agreement concluded with the subscriber;
- The IenW TSP determines that information in the certificate is incorrect or misleading;
- The IenW TSP ceases its activities and the CRL service is not taken over by another TSP;
- The technical content of the certificate creates an unacceptable risk for subscribers, relying parties and third parties (e.g. browser parties).

Revocation by the IenW TSP will always occur in the following circumstances:
- After being informed by the Municipal Database of the death of the certificate holder.
- After compromise of the private key of the IenW TSP or PKIoverheid. The certificates of all subscribers and certificate holders known to the IenW TSP will be revoked.
- If the card has not been collected within the prescribed period of 12 weeks [2].
- After definitive revocation or suspension of the BCT card.

The reason for each revocation carried out independently by the IenW TSP will be recorded by it.

The IenW TSP will ensure that the date and time of revocation of (services) certificates can be precisely determined. In case of doubt, the time determined by the IenW TSP will be the time of revocation. If a certificate has been revoked, it cannot be re-validated.

4.9.2 *Who may request revocation?*

The IenW TSP will revoke a certificate following an authorised request from the subscriber, the certificate holder or the certificate administrator. The IenW TSP may itself initiate a revocation request. A trusting party cannot make a request for revocation, but may report the suspicion of a circumstance that could lead to the revocation of a certificate. The IenW TSP will investigate such a report and, if there is reason to do so, will revoke the certificate.

4.9.3 *Procedure for requesting revocation*

Requests for revoking certificates may be made by telephone or electronically by an authorised person of the subscriber or by the certificate holder/certificate administrator. It should be noted that, if there is an urgent need for revocation, this must be done electronically via the website of KIWA (**https://intrekken.kiwabctkaart.nl**) must be done. This form of revocation is available twenty-four hours a day, seven days a week.

[2] In the period from the end of January 2020 up to and including April 10th 2020, revocation due to exceeding of the collection period was temporarily postponed during the large-scale replacement of the G2 BCT cards. Due to the corona crisis, this period has been extended to April 24, 2020.

For electronic revocation, the applicant must enter the card number of the on-board computer card to be revoked and the associated revocation code on the website of the IenW TSP. If the combination of revocation code and card number is correct, the certificates on the on-board computer card will be revoked. The applicant will be notified of this on the website. If the revocation code and card number are incorrect, a notification will be sent back stating that the revocation will not be executed. The IenW TSP has taken measures to prevent the making of unlimited erroneous revocation requests.

No documents will be supplied in the case of revocation by telephone. The person submitting the revocation request must answer a number of pre-determined questions. Based on these questions, the IenW TSP must obtain sufficient certainty about the identity of the party applying for the revocation and the on-board computer card for which revocation is being requested. After determining the identity of the party that submitted the revocation request and the on-board computer card, the IenW TSP will check whether the applicant is authorised to make the revocation request. After the checks have been carried out, the IenW TSP will revoke the certificates on the on-board computer card and will place them on the Certificate Revocation List (CRL). A confirmation of the completion or rejection of the request for revocation will be sent in writing to the subscriber and certificate holder.

The telephone revocation service is available during office hours on telephone number **088-9984888**.

A report by a trusting party of the suspicion of a circumstance that may lead to the revocation of a certificate may be made only by telephone.

The IenW TSP will ensure that the date and time of certificate revocation can be precisely determined. In case of doubt, the time determined by the IenW TSP will be the time of revocation. If a certificate has been revoked, it cannot be re-validated.

4.9.4 *Emergency procedure for a request for revocation*

If the website for electronic revocation is unavailable, the emergency procedure for a revocation request will take effect.

The party requesting revocation must send a revocation request by e-mail to the e-mail address **intrekkenBCT@kiwa.nl**. The applicant must include the following information in the revocation request:

- Card type;
- Card number;
- Revocation code;
- Reason for revocation;
- Name of the applicant, and;
- The telephone number where the applicant can be reached.

4.9.5 *Duration of processing of revocation request*

The maximum processing time for a revocation request is four (4) hours. In normal circumstances, the status change as a result of an electronic revocation or revocation by telephone will be processed in the next CRL, see section 4.9.7.

When using the emergency procedure KIWA will ensure that the revocation request is reported to KPN via the KPN Telephone Helpdesk within 1 hour by means of the

Major Incident procedure. KIWA will send the signed forms with the revocation information to KPN within 2 hours of receiving the revocation request. KPN has 3 hours after receiving the request and a further 2 hours after receiving the revocation information to execute the emergency revocation.

4.9.6 *Conditions for controls*

The control obligations of the relying parties are set out in paragraph 4.5.3 of this CPS and in the terms and conditions.

Revoked certificates will remain on the CRL even after expiry of the original validity date. This applies to certificates that have expired after October 1st, 2019.

4.9.7 *CRL issue frequency & maximum delay*

The CRL issuing frequency is once every three hours, with the CRL being valid for twenty-four hours. Not more than four hours after an authorised online request for revocation has been received, the IenW TSP will publish a CRL with the status change of the certificate.

If a card is revoked using the emergency procedure, the CRL will be published by the CA immediately after processing.

4.9.8 *Online revocation/status check*

Online Certificate Status Protocol (OCSP) will not be used in the user certificates, but is included in the G3 Services CA.

4.9.9 *Suspension of certificates*

The IenW TSP will not offer suspension of certificates.

4.10 Certificate Status Services

The status of certificates will be made known by the IenW TSP by means of a CRL. The CRL will be available 24 hours a day, 7 days a week. In the event of system defects or other causes beyond the control of the IenW TSP, the IenW TSP will do everything possible to ensure that the unavailability of the CRL does not last longer than four hours.

4.11 End of subscription ~~Termination of subscriber relationship~~

A subscriber that wants to cancel the subscription may contact the IenW TSP. Before the subscription can be terminated, the subscriber must revoke all certificates that have not yet expired.

4.12Key Escrow and ~~Key~~ Recovery

The private keys of the IenW TSP will not be given to a third party in key escrow.

The IenW TSP will not offer key recovery for the private keys related to issued certificates.

5 Facility, Management, and Operational Controls ~~Physical, procedural and personal security~~

The controls stated in Chapter 5 were determined based on the risk analysis and security plans for BCT card applications and issuance processes.

The implemented measures will guarantee shielded and well-protected registration, personalisation, certification, issuance and revocation processes to prevent unauthorised access to or breach of these processes or the locations where the processes are carried out.

5.1 Physical Security Controls

5.1.1 *Location*

The services of the IenW TSP will be performed by different parties and take place at different locations.

The registration activities and activities relating to the issuance and revocation of cards will take place at the location of the card issuer. The central registration system will be located in the computer centre of a specialised party.

The production of the on-board computer cards, i.e. the graphic personalisation and the generation of key material, will take place at the location of the personaliser.

The actual production of certificates will be carried out at the certificate producer's premises.

The issue of on-board computer cards will take place at the desired location of the *certificate holder / certificate manager. For this purpose, an appointment will be* agreed between the certificate holder / certificate manager and the distributor.

5.1.2 *Physical access control*

Appropriate physical security measures will be taken at all locations. These measures will be taken on the basis of risk analyses and security plans.

5.1.3 *Storage of media*

Storage media of the systems being used will be securely handled to protect the storage media from damage, theft, and unauthorised access. Storage media will be carefully destroyed when no longer needed.

5.1.4 *Waste disposal*

Measures will be taken at all locations to handle (confidential) waste in a safe manner.

5.1.5 *Backup outside the location*

Data necessary for guaranteeing the service provided by the IenW TSP in the event of an emergency will be adequately secured by the various parties.

5.2 Procedural Controls ~~security~~

5.2.1 *Trusted roles*

All positions that play a role in the provision of services within the IenW TSP will be designated as positions of trust, in accordance with the Implementing Regulations for Trusted Positions. The IenW TSP has at least the following designated officers:

- Trust Service Provider Manager (TSP-manager);
- Deputy Trust Service Provider Manager (dep. TSP-manager);
- Trust Service Provider Operational Manager (operational TSP-manager);
- Deputy Trust Service Provider Operational Manager (dep. operational TSP-manager).

5.2.2 *Number of persons required for each task*

Multiple employees will be required to perform certain predefined activities in the fields of key management, certificate management, system development, system maintenance and system management. The need to carry out a certain activity with multiple persons will be enforced among other things by means of technical facilities, authorisations in combination with identification/authentication and additional procedures.

5.2.3 *Segregation of duties*

The IenW TSP will apply a strict segregation between executive, decision-making, registering, saving and controlling duties. There will be a segregation of functions between system administration and operation of the TSP systems, as well as between security officer(s), system auditor(s), system administrator(s) and TSP operator(s).

5.3 Personnel Controls ~~al security~~

5.3.1 *Qualifications, experience and vetting*

The IenW TSP will engage sufficient personnel with sufficient professional knowledge, experience and qualifications necessary for the certification services. The knowledge, expertise and experience an employee must have for the position in question will be specified.

5.3.2 *Background check*

All employees involved in personalisation and certification work must be subject to vetting. The IenW TSP will require a Certificate of ~~Good Character~~Conduct from all employees subject to vetting.

The IenW TSP will conform to the provision contained in Article 24, paragraph 2 (b) of eIDAS concerning the recruitment of personnel. Personnel will not perform any work before they are formally employed. These same requirements will also apply to organisations to which the IenW TSP has outsourced activities.

5.3.3 *Educational requirements*

The educational requirements for employees will be laid down in the job descriptions. For each role there will be a description of what knowledge, expertise and experience the person must have.

5.3.4 *Sanctions for unauthorised acts*

After detection of an unauthorised action on a system, the employee who took the action will immediately be denied access to the system concerned. The responsible manager will decide the duration and conditions of the denial and the disciplinary measures to be taken.

5.3.5 *Hiring of external personnel*
The requirements stated in paragraph 5.3 apply in full to hired external personnel.

5.3.6 *Provision of documentation to personnel*
The job descriptions of the employees of the IenW TSP who operate the systems as an actor will be laid down in the Administrative Organisation and the accompanying work instructions.

5.4 ~~Procedures for a~~Audit Logging Procedures

5.4.1 *Recording of events*
Within the systems and applications used for the certification services, the events that are relevant to the quality of this service will be logged automatically or manually. These events will fall into different categories.

1. Registration operations in the card issuing system with regard to applying for on-board computer cards and any subsequent changes to the registration data;
2. Lifecycle events of keys of the CAs and of the keys produced by the IenW TSP for use by the BCT cardholders;
3. Lifecycle events of certificates and CRLs, including revocation requests and activities undertaken in response to those requests;
4. Lifecycle events of BCT cards;
5. Events in the infrastructure for certification services, including:
    - Breaches and attempted breaches of the systems;
    - Logging in and out by system administrators;
    - Actions by system administrators that are relevant to the reliability of the certification services;
    - Changes to authorisations (security profiles) and to accounts of actors;
    - Shutting down and (re)starting the systems;
    - Error messages from the hardware or software of the systems;
    - Installation of new or changed software;
    - Hardware changes;
    - Operations concerning the log files, log functionality, etc.

5.4.2 *Frequency of handling the audit log files*
Log files will be periodically analysed in accordance with the Management Protocols prepared for the certification service.

5.4.3 *Retention period of the audit log files*
The archiving system will save the archived audit log files for a period of at least seven years and will then delete them.

The archiving system will save the archived security log files for a period of at least 18 months and will then delete them.

5.4.4 *Protection of the audit log files*

Events that are recorded electronically and manually in audit log files will be protected against unauthorised access, alteration, deletion or other unwanted changes by means of physical and logical access controls.

5.4.5 *Backup procedures for audit log files*

By default, full backups will be made daily.

5.4.6 *Saving of audit logs*

The audit log files will be stored internally on the systems to which they relate. In addition, the logging will be archived off-site.

5.4.7 *Vulnerability analysis*

The IenW TSP will conduct a further investigation if the analysis of the audit log files indicates a possible malicious action or security incident.

5.5 Records Archival ~~Archiving procedures~~

5.5.1 *Types of archived data*

The IenW TSP will record all relevant registration information, including at least:

- The (certificate) application form;
- The data from/about the identity document shown by the certificate holder or certificate administrator;
- The findings and the decision on the application;
- The identity of the validation employee who handled or approved the certificate request;
- The method used to validate identity documents and to establish identities;
- The proof of identification and confirmation of receipt.

5.5.2 *Archiving retention term*

Paper forms and documents are scanned. The electronically archived data and the paper archives will be saved for at least seven years.

5.5.3 *Protection of archives*

The card issuer will use an appropriate system of measures for the protection of the archived data, in accordance with the GDPR and the Security Policy of the Ministry of Infrastructure and Water Management. This will include the following measures:

- The logging will be archived redundantly;
- The archive will be protected in respect of authenticity and integrity aspects;
- The audit trail will be provided with an electronic signature when archiving;
- Only a select group of employees will have access to the archive.

5.5.4 *Archive backup procedures*

By default, full backups will be made daily. No backup will be made of the paper archive

5.5.5 *Requirements for time-stamping of log records*

The log records will be provided with the date and time of the processing system on which the operation was performed. The processing systems will be synchronised with a reliable time source.

5.5.6 *Positioning of the archives files collection system*
The archiving system will be located in the card issuer's computer centre.

5.5.7 *Procedures for obtaining and verifying archived information*
The archiving system and the other important archives for the certification services will be accessible only by authorised employees.

5.6 Key Changeover ~~Procedures for renewing the TSP key~~

The generation and installation of the IenW TSP keys will take place in the certificate manufacturer's computer centre according to a predefined scenario.

5.7 Compromise and Disaster Recovery ~~Violation and continuity~~

5.7.1 *Procedures for handling incidents and violations*
Incidents will be reportable to the card issuer's call centre (**088-9984888**) and will be handled in accordance with regular incident management. If it is anticipated that an incident will escalate, an emergency will be reported to the IenW TSP. At that time, a decision may be made to let the business continuity plan of the IenW TSP take effect.

Compromising of the private key of the IenW TSP will be considered an emergency. In this situation, the IenW TSP will take at least the following actions:

- The IenW TSP will inform relying parties and BCT cardholders of the situation as soon as possible by publishing the information via the Internet;
- The IenW TSP will immediately revoke the relevant certificates and will publish them on the applicable CRL according to the normal publication schedule;
- The IenW TSP will initiate the Business Continuity Plan via the TSP.

5.7.2 *Recovery procedures for IT environments*
IT environments will be restored as part of incident management and the emergency plan of the IenW TSP. This will include a possibility to continue the service at fall-back locations.

5.7.3 *Recovery procedures for compromised keys of certificate holders*
Compromise of the keys of a BCT card or System card will lead to a revocation request as described. After revocation, a new card may be requested for which new keys will be generated.

5.8 CA or RA Termination ~~Termination of the TSP services~~

If the intention exists to terminate the certification service, the IenW TSP will do its best to ensure that the service is taken over within the Ministry itself or by another service provider under the hierarchy of the PKI for the government.

If this is not possible, the IenW TSP will inform the subscribers and certificate holders at least three months before the service is actually terminated. From that time onwards, KIWA will no longer issue BCT cards.

Upon termination of the certification service, KIWA will revoke all valid certificates and place them in the CRLs. The revocation status service with the CRLs will be maintained for at least six months after termination of the service.

No provisions have been made for the eventuality that the State of the Netherlands is no longer financially able to continue the certification services. However, see the provisions contained in 9.2, Financial responsibility and liability.

The IenW TSP will take all reasonably possible measures to limit the damage for BCT cardholders and relying parties and will ensure that there is still proof of certification that may be required in legal proceedings.

Concrete activities will be at least:

- Examining whether the taking over of the service by another registered trust service provider is possible;
- If this is possible, the issued qualified certificates will be transferred to this service provider;
- Informing subscribers, certificate holders and/or certificate administrators, relying parties and other parties with whom agreements have been concluded about the intended transfer or termination of the service;
- If transfer of the service is not reasonably possible:
    - Terminating the authorisations of subcontractors who are involved on behalf of the IenW TSP in providing certification services; this includes the breaking of external links;
    - All authorisations of subcontractors working on behalf of the IenW TSP in the process of issuing BCT certificates will be terminated.
    - Revocation of all valid certificates
    - Decommissioning or destroying the private keys in such a way that they can no longer be retrieved or put back into use.
    - Saving registration information, audit log files (archive, 7-year retention term) and CRLs in accordance with the prescribed requirements:
        - The retention term for registration information and audit log files can be found in the Statement of Requirements (Part 3, Basic requirements) under 5.4.3 PKIoverheid81.
        - The retention term for CRLs can be found in ETSI EN 319 411-2, under 7.3.6.i.

6 Technical Security Controls

6.1 Key Pair Generation and installation ~~of key pairs~~

The IenW TSP will use secure means and reliable systems to generate key pairs. The reliability and safety of these systems will always comply with internationally recognised standards and national legislation.

6.1.1 *Generation of key pairs*

When generating key pairs, the IenW TSP will use a reliable environment and the correct procedures that comply with recognised standards.

The generation of the key pairs for the (issuing) TSP CAs of the IenW TSP will take place in a FIPS 140-2 level 3 certified Hardware Security Module (HSM) at the location of the Certificate Producer. The keys of the key pairs will be 4096 bits asymmetrical RSA.

The key generation for the BCT cards and System cards will take place in a FIPS 140-2 level 3 certified HSM at the personaliser's location. The signature algorithm "sha256WithRSAEncryption" will be used for this purpose. The keys of the key pairs will be 2048 bits asymmetrical RSA. After receiving the certificates issued by the CA, the keys will be injected into the card (QSCD) using a secure communication channel that meets the requirements specified in ETSI EN 419 211 for Qualified Electronic Signature Creation Device (QSCD).

The IenW TSP will check the status of the QSCD every quarter as part of the life cycle management of the QSCD. The IenW TSP will switch to a replacement QSCD in time via regular management processes if the certification expires according to plan. If the QSCD certification expires prematurely and unexpectedly, the IenW TSP will inform the parties involved and come up with an alternative as quickly as possible.

6.1.2 *Transfer of private keys and QSCD to the user*

The cards with keys and certificates will:

- be handed over personally to the cardholder in the case of a Driver card or an Inspection card.
- The PIN and PUK code will be sent separately to the certificate holder in the form of a PIN mailer.
- Handed in person to a recorded employee of the subscriber in the case of a "non-registered" card (Business card, Control card and System card). The PIN code and PUK code will be sent separately to the certificate administrator in the form of a PIN mailer.

All keys will be provided via the card. Software-generated keys will not be processed.

6.1.3 *Transfer of public keys to the CA*

The key pairs for cards will be generated by the personaliser. The public key will be sent to the CA for processing using a secure connection by means of a signed production message.

6.1.4 *Transfer of the public key from the TSP to end-users*

The public keys of the (issuing) TSP CAs of the Ministry of Infrastructure and Water Management will be signed by the corresponding Domain Government CAs of the Policy Authority of PKIoverheid. This signing will assure the integrity and origin of these public keys.

The above keys will be made available in the form of a certificate via the issued cards and the website.

6.1.5 *Key lengths*

The key length for certificates for BCT cards is 2048 bits RSA. The certificates of On-board Computer Cards will be signed by the "MinIenW PKIoverheid Organisatie Persoon CA - G3" or "MinIenW PKIoverheid Organisatie Services CA - G3" with a key length of 4096 bit RSA.

The key length for certificates for System cards is 2048 bits RSA. The System cards will be signed with the "MinIenW PKIoverheid Autonome Apparaten CA - G3" with a key length of 4096 bit RSA.

6.1.6 *Hardware/software key generation*

Keys will only be generated in hardware.

6.1.7 *Objectives of key use (within the meaning of X.509 v3)*

The certificates, including the associated key pairs, will be intended solely for the purposes described in this CPS. The purposes for which a key may be used will be included in the certificate. The KeyUsage and Extended KeyUsage attributes will be included in the certificate for this purpose.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 *Standards for cryptographic modules*

For operational use, the cryptographic data will be stored in a Hardware Security Module (HSM). The HSM will meet the requirements described FIPS 140-2 level 3 or higher.

6.2.2 *Segregation of functions for private key management*

Access to the HSMs and thus the private keys of the CAs will be restricted to holders of a trusted role, where necessary on the basis of the dual control principle.

A backup will additionally be made of the private keys of the CAs of the IenW TSP. The backup will be stored in multiple encrypted parts in cryptographic modules. The backup may only be used when the holders of these modules are present with their part of the key.

The private keys of the CAs will not be externally escrowed by the IenW TSP.

6.2.3 *Escrow of private keys of cardholders*

The IenW TSP will not offer escrow services to cardholders.

6.2.4 *Backup of the private keys of certificate holders*

The IenW TSP will not back up the private keys of certificate holders.

6.2.5 Archiving of private keys of certificate holders

Private keys of certificate holders will not be archived. Technical and organisational measures will be taken to ensure that it is not possible to archive these keys.

6.2.6 Access to private keys in cryptographic module

The IenW TSP CAs will securely save their own private keys in an HSM for the entire lifecycle in such a way that use is possible only under dual control.

The BCT cards and System cards will also contain private keys. Access to them will be blocked by means of a PIN.

6.2.7 Storage of private keys

The private keys of the IenW TSP CAs will be stored encrypted in an HSM. Access security will be used to ensure that the keys cannot be used outside the module.

The private keys of certificate holders will be stored on the card in such a way that they can be used only on the card. During the production process, the personaliser has the generated version of the private keys of the certificate holder, see also section 6.1.1 *Generating key pairs*. Technical and organisational measures make unauthorised use of these private keys impossible and ensure that they only become available to the certificate holder in usable form. The personaliser destroys immediately after dispatch -but no later than 10 working days after generating a key pair- every copy of the private keys from its systems.

6.2.8 Activation of private keys

The private keys of the (issuing) TSP CAs of the IenW TSP will be activated only by means of a key ceremony with the necessary employees present. The IenW TSP will ensure there is a careful procedure in a secure environment.

An activation code (PIN) will be provided to activate end-user private keys.

6.2.9 Method for deactivating private keys

The private keys used by the IenW TSP CAs to issue certificates will not normally be deactivated. These keys will remain in production in a secure environment.

6.2.10 Method for destroying private keys

The private keys used to sign certificates will no longer be usable after the end of their lifecycle. The IenW TSP will ensure there is adequate destruction, making it impossible to deduce the destroyed keys from the remnants.

6.2.11 Secure means for creating electronic signatures

Hardware Security Modules used within the systems of the IenW TSP will be certified in accordance with FIPS 140-2 level 3. As a result, cryptographic material cannot be changed unnoticed during storage, use and transport. The HSMs will be delivered by the manufacturer in packaging that makes visible any form of corruption of the contents.

The complete QSCD of the BCT card and System card will be independently certified against the Common Criteria for Security Evaluation standard. The applicable guarantee level will be EAL5+. The basic principle is that this QSCD certification will be valid for the entire duration of use of the BCT card.

6.3 ~~Additional~~ Other Aspects of Key Pair Management

All key management matters will be carried out by the IenW TSP by applying careful procedures that are in accordance with the intended purpose.

6.3.1 *Archiving of public keys*
Public keys will be archived by the IenW TSP for a period of at least seven years after expiry of the original period of validity of a certificate. This archiving will take place in the physically safe environment of the CA.

6.3.2 *Duration of use of public/private key*
The key pairs and certificates used by the IenW TSP will in all instances be valid for 1 day less than the parent CA. As a result, the Ministry of Infrastructure and Water Management TSP CAs will be valid for one day less than the end of the validity of the parent domain CA of PKIoverheid.

For the certificates on the BCT cards, including the corresponding key pairs, reference is made to paragraph 1.1.2.

6.4 Activation data

6.4.1 *Generation of activation data*
Activation data will be required in order to use the private key on the card. This data will consist of a PIN and a PUK code. The activation data will be created securely by the personaliser when the key pair is created.

The PIN will consist of at least four digits and the PUK code of twelve digits in all cases, while the PUK code for System cards will consist of 64 characters. The PIN code and the PUK code will be made available only to the certificate holder.

6.4.2 *Protection of activation data*
The activation data will be distributed in such a way that it is impossible for third parties to become knowledgeable of the data unseen. A PIN mailer will be used for this purpose. The distribution of the PIN mailer will always occur separately from the card. After transfer of the activation data, the certificate holder will be responsible for the protection of the data.

The card will block after the sixth entry of an incorrect PIN code. The card can be unblocked by means of the PUK code. Hereby, a new PIN will be selected. If the PUK code has been entered incorrectly three times, the BCT card will be permanently blocked and thus rendered unusable.

6.5 Computer Security Controls ~~Access protection of TSP systems~~

6.5.1 *General system security measures*
The IenW TSP will have an information security policy and, in accordance with the policy, will take measures to guarantee the availability, integrity and exclusivity of the systems used. Computer systems will be appropriately protected against unauthorised access and other threats. The measures will be set down in detail with the various operational parties in Service Level Agreements (SLAs). Management work will be logged.

6.5.2 *Specific system security measures*
Appropriate controls and security measures will be incorporated in the registration systems of the IenW TSP, with adherence at least to the level required in the Statement of Requirements of PKIoverheid. Partly thanks to these steps, it will be impossible for only one employee of the IenW TSP to deal with a card application.

6.5.3 *Management and classification of resources*
The IenW TSP will classify the resources used on the basis of a risk analysis.

6.6 ~~Technical L~~ifecycle Security Controls

6.6.1 *System development controls*
For the systems developed by the IenW TSP, an accredited EDP auditor will issue an audit report based on CEN TS 419 261. The IenW TSP will perform tests before systems are put into use. These tests will be conducted on the basis of predetermined test plans.

6.6.2 *Security management controls*
The IenW TSP will have separate test/acceptance and production systems. The transfer of software from one environment to another will take place in a controlled manner using a change management procedure. This procedure will include updating and recording versions, changes and emergency repairs of all operational software.

The integrity of the systems and information of the IenW TSP will be protected against viruses, harmful and unauthorised software and other possible sources that may lead to service disruption by means of a combination of appropriate physical, logical and organisational measures. These measures will be of a preventative, deterrent and corrective nature. Examples of measures are: logging, firewalls, intrusion detection and redundancy of systems, system components and network components.

It is additionally mandatory to follow security issues in the market and to keep all software and hardware up to date. This means that no use may be made of software and hardware that is no longer provided with security updates. However, it is recommended to implement all available new versions that are released to improve system security.

The various operational parties will be personally responsible for correctly applying the necessary measures within the scope of their own services and must have a test/acceptance and production system.

Storage media of the systems used will be securely handled to protect the storage media from damage, theft, and unauthorised access. Storage media will be carefully removed when they are no longer needed.

6.6.3 *Security classification lifecycle*
Classification will be assessed periodically and adjusted if necessary.

6.7 Network Security Controls

The availability, integrity and exclusivity of the data exchanged between the various operational parties will be guaranteed by means of network security measures. Communication over public networks between systems of the operational parties will take place in confidential form. The link between on the public networks on the one hand and the networks of the card issuer, personaliser and certificate producer on the other will be provided with stringent security measures (current firewall, virus scanners, proxy).

6.8 Timestamping

The IenW TSP will not offer timestamping services to third parties.

7 Certificate, ~~and~~ CRL, and OCSP Profiles

7.1 Certificate Profile~~s~~

The certificates issued for use on the BCT cards and System cards will comply with the profiles in the current version of the document headed “MinIenW TSP PKIoverheid Certificaatprofielen BCT G3”.

7.2 CRL Profile

The profile of the CRL issued by the IenW TSP is described in the current version of the document headed “MinIenW TSP PKIoverheid Certificaatprofielen BCT G3”.

7.3 OCSP Profile

Online Certificate Status Protocol (OCSP) will not be used in the user certificates, but is included in the G3 Services CA.

8 Compliance Audit and Other ~~Conformity~~ Assessment

The TSP service provisioning of the Ministry of Infrastructure and Water Management has been certified at the level of Scheme for certification of Certification Authorities to ETSI EN 319 411-2 and ETSI EN 319 411-1 and thus meets the requirements set for Trust Service Providers (both in combination with ETSI EN 319 401).

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS (NetSec)

Explanatory notes
The network and certificate system security requirements (Requirements) will apply to all publicly trusted certification authorities (CAs) and will have been approved with the intention of ensuring that all such CAs and Delegated Third Parties are checked for compliance.

With regards to these requirements, the CA will be responsible for all tasks performed by delegated third parties.

Regulation on Electronic Identities and Trust Services (eIDAS)
On 1 July 2016, the European Regulation (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) entered into force. This Regulation replaces the Electronic Signature Act.

The Ministry of Infrastructure and Water Management also complies with the relevant parts of the Statement of Requirements of the PKIoverheid as set out in the Statement of Requirements (see https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen). This can be demonstrated by means of audit report issued by BSI Group The Netherlands B.V.

A copy of the ETSI EN 319 411-1 and the ETSI EN 319 411-2 certificate can be found on the website of the IenW TSP (https://bct.tsp.minienw.nl/).

The audit reports prepared by the relevant auditors will be kept secret for security reasons. They will not be made available to third parties and may be viewed only on request and subject to strict confidentiality.

With effect from 10 March 2017, Telecommunications Agency Netherlands (hereinafter 'AT') was designated as the statutory supervisor of the eIDAS Regulation. That is why certification is also against eIDAS Regulation (electronic identification and trust services for electronic transactions).
The Trust Service Provider of the Ministry of Infrastructure and Water Management is certified for ETSI EN 319 411-1 and ETSI EN 319 411-2).

8.1 Audit cycle

The Implementing Act for the eIDAS Regulation states, among other things, the frequency for performing the audit, the requirements the certification body must meet and how non-conformities must be dealt with. A certification body must be accredited by a member of IAF (International Accreditation Forum) in accordance with ISO 17065 before being able to certify.

The audit cycle will be performed according to the ETSI EN 319 403 certification scheme. The IenW TSP will undergo a certification audit once every 2 years. A full audit will be carried out in the intervening year. If larger changes are made at policy or technical level, an interim compliance audit may be carried out.
In addition to these audits, the IenW TSP will have internal audits conducted.

The IenW TSP will oversee, partly via the card issuer, the operational parties that jointly provide the services.

8.2 Certification body

Certification audits and control audits will be performed by an accredited organisation. This organisation must be accredited by a member of IAF (International Accreditation Forum) in accordance with ISO 17065.

8.3 Relationship with certification body

The auditors who perform the audits will be independent. There will be no further relationship between the Ministry of Infrastructure and Water Management and the certification body.

8.4 Subject of audit

During the audits, there will be an assessment of whether the issue of (qualified) certificates continues to meet the requirements contained in the standards:

- ETSI EN 319 411-1, (for the Business card, Control card and System card not registered in a name), including the standards referred to herein in the CABforum Baseline Requirements and the Network Security Controls.
- ETSI EN 319 411-2, (for the Driver card and Inspection card registered in a name)
- Requirements from the Electronic Identities and Trust Services Regulation (the eIDAS Regulation)
- The Statement of Requirements PKIoverheid Parts 3a, 3b and 3d.

The audit will be performed in respect of the following matters and processes:

- Registration Service;
- Certificate Generation Service;
- Dissemination Service;
- Revocation Management Service;
- Subject Device Provision Service;
- Revocation Status Service.

8.5 Audit Results

If any shortcomings are found during the audit, the IenW TSP will prepare an action plan within 15 days of receipt of the final audit report in order to analyse the identified non-conformities and to take effective corrective measures.

8.6 Availability of conformity certificates

The certificates of conformity of the most recent audits will be available on the website of the Trust Service Provider (BCT) and in the electronic repository of the Policy Authority of the PKI for the government. The IenW TSP will also comply with the standards framework of the PKI for the government as set down in the Statement of Requirements (see https://www.logius.nl).

9 Other Business and ~~General~~ Legal Matters ~~provisions~~

The Ministry of Infrastructure and Water Management is the ultimately responsible trust service provider and is also responsible for the parts outsourced to other organisations. The Human Infrastructure and Transport Inspector, as the IenW TSP, has outsourced the actual card issuing to Kiwa Register B.V. The personalisation of the BCT cards and the creation of the key pairs will be handled by IDEMIA The Netherlands B.V., while the production of the certificates has been outsourced to KPN B.V.

9.1 Fees ~~Tariffs~~

No tariffs are included in this CPS. Information about the tariffs can be found in the "Regulation on payments for documents under the Passenger Transport Act 2000".

9.2 Financial responsibility ~~and liability~~

The IenW TSP will make adequate arrangements to cover liabilities related to the present service. The recoverability of liability claims relating to this service will be guaranteed by the financial position of the ~~DHI BCT, the~~ Ministry of Infrastructure and Water Management and in a wider context the State of the Netherlands (Central Government).

The IenW TSP has not taken out a separate insurance policy for certification services. After all, it is government policy that the State does not insure itself.

See section 9.6 for liability.

9.3 Confidentiality of Business Information ~~data~~

Anyone can submit a request to the IenW TSP to submit documents under the Government Information (Public Access) Act.

When assessing a request for disclosure of documents, a check will be made against provisions contained in Government Information (Public Access) Act.

9.4 ~~Confidentiality~~ Privacy of Personal Information ~~data~~

All performed actions that are important in the registration process will be recorded. As few personal data as possible will be recorded. No (personal) data will be recorded that is not relevant to the registration process.

The certificate holders have the right to inspect and correct their personal data. The certificate holder may also check with the IenW TSP whether anybody viewed the data and, if so, who.

9.4.1 *Confidential information*

The information obtained by the IenW TSP about a person, i.e a natural person or a legal person, will be treated confidentially. The requirements contained in the General Data Protection Regulation (GDPR) will expressly apply in this regard.

At least the following documents contain information that is considered confidential and will not therefore be provided to third parties:

- Information for the registration and certification of parties;
- Agreements with suppliers and service providers;
- Security procedures and measures;
- Audit reports.

9.4.2 *Non-confidential information*

The content of certificates is freely consultable. However, the certificates issued by the IenW TSP will not be published. The information contained in a certificate and provided with regard to revoked certificates will be confined to what is stated in Chapter 7, "Certificate, CRL and OCSP profiles" of this CPS.

Information regarding the revocation of certificates will be available via the CRL. The CRL will contain only information about revoked certificates. The information given in the list will concern, for each certificate, the certificate number, the time of revocation, the reason for revocation and optionally the probable time when the revocation reason arose.

9.4.3 *Release of information*

If in the context of a criminal or disciplinary investigation, non-public information from the IenW TSP registration is requested by a competent investigating officer, the information will be released by the IenW TSP. The requirements contained in GDPR will expressly apply to this information.

If non-public information is requested from the IenW TSP registration by a subscriber or certificate holder in civil proceedings for the purpose of providing proof of certification, this information will be released by the IenW TSP, if, in its opinion, there is no compelling interest that precludes the provision of the data. If data will be provided, the data subject will be informed.

Confidential data will only be provided for evidence to parties other than the subscriber or certificate holder with the prior written consent of the subscriber or certificate holder.

Except for the aforementioned instances, no data belonging to certificate holders or subscribers will be released to third parties, unless permissible from further legislation and regulations or unless the subscribers or certificate holders have given their explicit consent.

9.5 Intellectual Property Rights

This CPS is owned by the IenW TSP. Unaltered copies of this CPS may be distributed and published without permission provided that this is done with acknowledgement of the source.

Property rights attached to certificates, BCT cards and System cards will remain vested in the State of the Netherlands, including intellectual property rights, even after they have been issued.

The IenW TSP will guarantee its subscribers, certificate holders and administrators that the certificates and carriers of the private and public keys issued by it, including the associated and supplied equipment and documentation, do not infringe intellectual property rights, including copyrights, trademark rights and software of which the rights are held by its suppliers.

9.6 Representations and Warranties

No stipulation.

9.7 Disclaimers and warranties ~~Liability and guarantees~~

The PKIoverheid Certificates Terms and Conditions set out how the IenW TSP and the parties involved will deal with ~~liability~~ disclaimers and warranties.

9.8 Limitations of Liability ~~in warranties~~

The PKIoverheid Certificates Terms and Conditions set out how the IenW TSP and the parties involved will deal with limitations of liability ~~in warranties~~.

9.9 Indemnities~~fication~~

No~~/a~~ stipulation.

9.10 ~~CPS validity~~ Term and Termination

The CPS will be valid from the date of publication. The CPS will be valid as long as the service of the IenW TSP continues or until the CPS is replaced by a newer version.

If one or more stipulations of this CPS are declared inapplicable by legal judgement or otherwise, this will not affect the validity and applicability of all other stipulations. In that case the parties will be bound by a stipulation with the same purport, wherever possible, which cannot be rendered invalid.

Newer versions will be published via the electronic repository, as described in Chapter 2.

9.11 Individual notices and communication with participants ~~involved parties~~

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The currently valid CPS will be assessed and updated by IenW TSP at least annually. Changes apply as of the moment that the new CPS is published.

The IenW TSP always offers a modified CPS version for approval by the TSP management.

9.12.2 Change and classification requests

The IenW TSP has the right to make amendments and/or additions to the CPS.

Subscribers, certificate holders, certificate administrators and relying parties can make comments and observations about the content of the CPS and submit them to the IenW TSP. The contact details of the IenW TSP are stated in paragraph 1.5.1. If the IenW TSP, possibly in consultation with the TSP, determines that changes need to be made to the CPS based on comments and observations, those changes will be implemented.

The IenW TSP will classify the change requests. Where necessary, specialist legal or technical knowledge will also be consulted. During classification the urgency of the change request will also be determined.

When changing the CPS, the impact will be determined for the enforcement application of ILT. If necessary, timely alterations can then be made here.

Changes of a textual nature or corrections of writing and/or spelling errors can take effect without prior notice and will be recognisable because the version number will have been increased by 0.1.1. The PKIoverheid version number will be used for changes to the Statement of Requirements sections.

9.12.3 Publication of changes

After approval the new version of the CPS will be published on the website of the IenW TSP.

9.13 Dispute Resolution Procedures

The IenW TSP will have a complaints procedure and an objection and appeal procedure.

Objections against a decision on the issue of a BCT card or System card may be addressed to:

Human Environment and Transport Inspectorate
For the attention of Objection and appeal
PO Box 16191
NL-2500 BD The Hague

Other complaints about the service may be addressed to:

Kiwa Register B.V.
For the attention of the Quality Team
PO box 4
2280 AA, Rijswijk (ZH)
E-mail: **NL.Wegvervoer@kiwa.nl** ~~vergunningen@kiwa.nl~~
Telephone: +31 88 9984888

9.14 ~~Applicable~~ Governing Law

Dutch law will govern the services of the IenW TSP, the present CPS and agreements concluded by the IenW TSP on account of the certification services.

9.15 Compliance with Applicable Law ~~relevant legislation~~

The IenW TSP will comply with the relevant legislation in the letter and spirit of the law.

9.16 Micellaneous Provisions

No stipulation.

9.17 Other provisions

No stipulation.

10 Revisions

10.1 Revision 4.8.1 G3 EN → 4.8.2 G3 EN

4.8.2 G3 EN	July 13th, 2020	Changes: o The CPS of the TSP MUST follow the classification according to RFC 3647. All sections and subsections as defined in RFC3647 MUST be included in the CPS. Empty sections are not allowed. o Mail address KIWA permits changed from vergunningen@kiwa.nl to NL.Wegvervoer@kiwa.nl. o Par. 4.9.1 the footnote relating to the suspension of the collection period has been removed.

10.2 Revision 4.8 G3 EN → 4.8.1 G3 EN

4.8.1 G3 EN	April 3rd, 2020	Temporary change: o Par. 4.9.1: updated footnote concerning 12 week collection period. Period extended until April 24, 2020 due to the corona crisis.

10.3 Revision 4.7.4a G3 EN → 4.8 G3 EN

4.8 G3 EN	February 7th, 2020	Changes: o a distinct 'Dossierhouder BCT' role is no longer present; all tasks carried out by 'IenW TSP' accommodated at the Human Environment and Transport Inspectorate (ILT); o H1 introductie: added IenW TSP description; o Par. 1.5.1: Update contact information; o Par. 1.3.3: Card issuer uses multi-factor authentication; o Par. 3.3.1: Added reference to shortening rules for commonName, givenName and surname; o Terminology: 'Certificate Service Provider' replaced by 'Trust Service Provider' also in Definitions; o Par. 3.2.6: added to align with RFC 3647; o Par. 4.4: extended to align with RFC 3647; o Par. 5.2.1: added designated officers (roles).

10.4 Revision 4.7.4 G3 EN → 4.7.4a G3 EN

4.7.4a G3 EN	January 27th, 2020	Temporary change: o Par. 4.9.1: added footnote concerning 12 week collection period.

10.5 Revision 4.7.3 G3 EN → 4.7.4 G3 EN

4.7.4 G3 EN	December 9th, 2019	Changes to follow up audit findings: o Removed numbering heading 3.1.2, added par. 3.1.6 to comply with RFC 3647 based on review comments KIWA; o Par. 3.4: clarification of authentication using revocaction by telephone; o Par. 4.1.2: supplier → card issuer;

		o Par. 4.1.1, 4.1.2 and 4.3 clarified signing for acceptance of CPS and Terms and conditions and being held to regulation based on review comments KIWA; o Par. 4.1.3: clarified 'same period of validity' based on KIWA review comments; o Par. 4.3: clarified issuance control cards, business cards and system cards to certificate manager; o Par. 4.3: clarified doorstep process based on review comments AMP; o Par. 4.5.3: 'trusting party conditions' → 'Terms and Conditions'; o Par. 4.9.5 clarified processing time of revocation regular procedure and emergency procedure; o Par. 4.9.6: added starting date for keeping expired certificates listed on CRL; o Par. 5.1.1 location of issuance described for all on-board computer cards; o Par. 5.5.2: added scanning paper documents; o Par. 6.1.1: added QSCD monitoring procedure; o Par. 6.2.7: clarification of private key protection during production process; o Par. 4.6.5 and 5.8: consistent referencing to 'KIWA'; o Par. 9.11 added approval process for CPS by TSP management.

10.6 Revision 4.7.3 G3 EN

4.7.3 G3 EN	October 2nd, 2019	First English version.

Bijlage A Definitions

Term	Definition
Applicant	a natural person (Professional Certificates) or a legal person (Organisational Certificates) who submits a Certificate application for the issue of a Certificate to the IenW TSP. The Applicant does not have to be the same party as the Subscriber or the Certificate Holder, but does have to be one of them.
Subscriber	the natural person (Professional Certificates) or legal person (Organisational Certificates) who enters into an agreement with the IenW TSP to bring about the issue of PKIoverheid Certificates to Certificate Holders designated by the Subscriber.
Key pair	a Public Key and Private Key within public key cryptography that will be mathematically linked to each other in such a way that the Public Key and the Private Key are each other's counterpart. If one key is used for encryption, the other must be used for decryption and vice versa.
Authentication	(1) checking an identity before information is transferred; (2) checking the correctness of a message or sender.
Authentication certificate	Certificate certifying the Public Key of the Key Pair used for identification and authentication services.
Autonomous Device Certificate	a Non-Qualified Certificate stored on a QSCD that supports the function of authentication and is issued only to devices that independently guarantee the integrity and authenticity of (measurement) data in their operational life for (a specific purpose within a core task of) a certain government authority. The Certificates will meet the following requirements: a) they were issued for a device mentioned above, and; b) they were issued on the basis of the 'Certificate Policy Domain Autonomous Devices' applicable within the PKIoverheid.
Professional Certificate	a combination stored on a QSCD of a Non-Qualified Certificate that supports the function of authentication, and a Qualified Certificate that supports the function of Irrefutability, and that will be issued exclusively to a practitioner of a Recognised Profession. The Certificates will meet the following requirements: a) they were issued to a natural person who uses or is about to use the Certificate for the purpose of his/her profession, and; b) they were issued on the basis of the 'Certificate Policy Domain Government/Companies and Organization'.
Authorised Representative	The representative of the Subscriber who is authorised to represent the Subscriber in matters concerning Certification Services.
CA Certificate	a Certificate of a Certification Authority.
CA keys	the Key Pair, the Private Key and the Public Key of a Certification Authority.
Certificate	the Public Key of an End-User, together with additional information. A Certificate will be encrypted with the

Term	Definition
	Private Key of the Certification Authority that issued the Public Key, making the Certificate impossible to falsify.
Certificate application	the request submitted by an Applicant for the issue of a Certificate by the IenW TSP.
Certificate Administrator	a natural person who is authorised to request, install, manage and/or revoke a Certificate on behalf of the Subscriber and for the Certificate Holder. The Certificate Administrator performs actions that the Certificate Holder personally is unable to perform.
Certificate Holder	an entity identified in a Certificate as the holder of the Private Key associated with the Public Key given in the Certificate.
Certificate profile	a description of the content of a Certificate. Each type of Certificate (signature, confidentiality, etc.) has its own embodiment and therefore its own description - this includes, for example, arrangements regarding names and similar.
Certificate Policy (CP)	a named set of rules that indicates the applicability of a Certificate for a specific community and/or application class with common security requirements. By means of a CP, Subscribers and Relying parties can determine how much trust they can place in the relationship between the Public Key and the identity of the holder of the Public Key. The applicable CPs will be included in the Statement of Requirements of the PKIoverheid. This concerns the part 3a Certificate Policy - Domain Government / Companies and Organisation, the part 3b Certificate Policy - Services and the part 3d Certificate Policy - Autonomous Devices, appendices to CP Domain Government/Companies and Organisation
Certificates Revocation List (CRL)	a publicly accessible and consultable list of revoked Certificates, signed and made available by the issuing TSP CA.
Trust Services	the issue, management and revocation of Certificates by Trust Service Providers.
Certification Practice Statement (CPS)	a document describing the procedures and measures taken by a TSP with regard to all aspects of the service. The CPS thus describes how the TSP meets the requirements stated in the applicable CP.
Certification Practice Statement PKIoverheid (CPS PKIoverheid)	the present CPS, as applicable to issue by the IenW TSP of PKIoverheid Certificates and their use.
Trust Service Provider (TSP)	a natural or legal person who issues certificates or provides other services related to electronic signatures. The TSP's function is to provide and manage Certificates and key information, including the provided carrier (QSCD). The TSP also has ultimate responsibility for providing the Trust Services, regardless of whether it performs the actual work itself or outsources it to others. The procedures and measures taken by the TSP with regard to all aspects of the Public Key Infrastructure (PKI) are described in the Certification Practice Statement (CPS).
End-User	a natural or legal person who fulfills one or more of the following roles within the PKIoverheid: Subscriber, Certificate Holder or Trusting Party.

Term	Definition
Electronic Signature	electronic data that is attached to or logically associated with other electronic data and that is used as a means of authentication. By placing an Electronic Signature, it is assured that someone who claims to have signed a document has actually done so.
Electronic Storage	location where relevant information about the services of the IenW TSP can be found.
Recognised profession	In the case of professional Certificate Holders, they must practice a recognised profession to be able to apply for Certificates within the PKIoverheid. A recognised profession as used here means a profession involving: · a (professional) register recognised by the relevant professional group, with a legally regulated disciplinary code and where registration in the register is mandatory to be allowed to practice the profession; · legal requirements for practicing the profession, with valid proof (such as a licence) must be obtained to be allowed to practice the profession.
Escrow (Key-Escrow)	A method to generate a copy of the Private Key during the issue of a Certificate for access to encrypted data by authorised parties, as well as the secure storage thereof.
Data for creating Electronic Signatures	see Signature Creation Data.
Data for verifying an Electronic Signature	see Signature Verification Data.
Qualified Certificate	a Certificate that meets the requirements set under Section 18.15, second paragraph of the Telecommunications Act, and is issued by a Trust Service Provider that meets the requirements set under Section 18.15, first paragraph of the Telecommunications Act. The Certificate must also allow use of the Qualified Electronic Signature.
Qualified Electronic Signature	an Electronic Signature that meets the following requirements: a) it is uniquely linked to the signer; b) it makes it possible to identify the signer; c) it is created with tools that the signer can keep under his exclusive control; d) it is linked in such a way to the electronic file to which it relates that any subsequent changes to the data can be traced; e) it is based on a Qualified Certificate within the meaning of Section 1.1, part dd of the Telecommunications Act; f) it is generated by a secure tool for creating Electronic Signatures within the meaning of Section 1.1, part gg of the Telecommunications Act.

Term	Definition
Group Certificate	a combination of two Non-Qualified Certificates stored on a QSCD that together support the functions of confidentiality and authentication and that meet the following requirements: a) they were issued to a service or a function that is part of the Subscriber (organisational entity), and b) they were issued on the basis of the Certificate Policy Services applicable within the PKIoverheid.
Hardware Security Module	The peripheral used on the server side to speed up cryptographic processes. In particular, this relates tor the creation of keys.
Safe tool for creating Electronic Signatures	see Qualified Signature Creation Device (QSCD).
Non-Qualified Certificate	a Certificate that does not meet the requirements for a Qualified Certificate.
Object Identifier (OID)	a row of numbers that uniquely and permanently identifies an object.
Online Certificate Status Protocol (OCSP)	a method to check the validity of Certificates online (and in real time). This method can be used as an alternative to consulting the CRL.
Non-repudiation	the property of a message to show that certain events or actions have taken place, such as sending and receiving electronic documents.
Organisational Certificate	a combination of two Non-Qualified Certificates stored on a QSCD that together support the functions of authentication and confidentiality, as well as a Qualified Certificate that supports the function of Non-repudiation, and which meet the following requirements: a) they were issued to a natural person who uses or will use the Certificate on behalf of the Subscriber (organisational entity), and b) they were issued on the basis of the 'Certificate Policy Domain Government/Companies and Organization' applicable within PKIoverheid.
Policy Authority of PKIoverheid	the highest policy-making authority within the hierarchy of the PKIoverheid that orchestrates the Root CA.
Personal Certificate	a certificate issued to a Natural Person. A distinction is made between Organisational and Professional Certificates. In the case of Organisational Certificates, the Certificates are requested by an organisational entity, which is a Subscriber with the IenW TSP, for a Certificate Holder that is part of or maintains a relationship with that organisational entity. The Certificate Holder uses the Certificate on behalf of the organisation. In the case of Professional Certificates, they are requested by a practitioner of a Recognised Profession, who in that capacity is himself a Subscriber, but at the same time also a Certificate Holder. The Certificate Holder uses the Certificate for the purpose of his profession.
PKI for the government, the Public Key Infrastructure of the State of the Netherlands (also known as PKIoverheid)	a set of arrangements that allows generic and large-scale use of the Electronic Signature, and also facilitates remote identification and confidential communication. The set of arrangements is owned by the Minister of the Interior and Kingdom Relations and is managed by the PKIoverheid Policy Authority.
PKIoverheid Certificate	a Certificate issued by the IenW TSP under the PKIoverheid

Term	Definition
Policy Management Authority	the organisational entity within the IenW TSP that is responsible for developing, maintaining and formally laying down documents related to the service, including the CPS.
Private key	see Private Key.
Private key	the key of a Key Pair that must be known only to its holder and must be kept strictly secret. Within the framework of the PKIoverheid, the Private Key is used by the Certificate Holder to identify himself electronically, to place his Electronic Signature or to decipher an encrypted message.
Public key	see Public Key.
Public Key Infrastructure (PKI)	the entire organisation, procedures and technology required for issuing, using and managing Certificates.
Public key	the key of a Key Pair that may be publicly disclosed. The Public Key is used to check the identity of the owner of the Key Pair, to check the Electronic Signature of the owner of the Key Pair and to encrypt information for a third party.
QSCD	A QSCD is a Secure Signature Creation Device that is certified and approved for the generation of Qualified Electronic Signatures (QES). It uses technical and procedural tools to ensure that: - Signature keys are kept secret - Signature keys are made using established cryptographic techniques. - Signature keys can be used only by the correct owner. - Compliance with strict standards for QES. A QSCD may be a smart card or a USB token, for example.
Regulations for use of On-board computer and On-board computer cards	The regulations applicable to all parties involved in the issue and use of PKIoverheid Certificates.
Root	the central part of a (PKI) hierarchy in which the entire hierarchy and its reliability level is embedded.
Root Certificate	see Root Certificate
Root Certification Authority (Root CA)	a CA that is the centre of common trust in a PKI hierarchy. The Certificate of the Root CA (the Root Certificate) is self-signed, so it is not possible to authenticate the source of the signature on the Certificate, only the integrity of the contents of the Certificate. However, the Root CA is trusted on the basis of, for example, the CP and other documents. The Root CA does not necessarily have to be positioned at the top of a hierarchy.
Services Certificate	see Group Certificate.
Signature Creation Data	unique data, such as codes or private cryptographic keys, that are used by the signer to create an Electronic Signature.
Signature Creation Device	configured software or hardware that is used to implement the data for creating Electronic Signatures.
Signature Verification Data	data, such as codes or cryptographic Public Keys, that are used to verify an Electronic Signature
Key Pair	unique combination of Private Key and Public Key

Term	Definition
Root Certificate	the Certificate of the Root CA. This is the Certificate belonging to the place where trust in all Certificates issued within the PKIoverheid originates. There is no higher-ranking CA from which trust is derived. This Certificate is signed personally by the Certificate Holder (within the PKIoverheid that is the Government CA). All lower-ranking Certificates are issued by the holder of the Root Certificate
Secure tool for creating Electronic Signatures	see Secure Signature Creation Device.
Confidentiality Certificate	Certificate certifying the Public Key of the Key Pair used for confidentiality services.
Relying Party	the natural or legal person who is the recipient of a Certificate and who relies on that Certificate.
X.509	an ISO standard that defines a basis for the electronic preparation of Certificates.

Bijlage B Acronyms~~Abbreviations~~

Abbreviation	Meaning
AP	Dutch Data Protection Authority
AT	Telecommunications Agency Netherlands
GDPR	General Data Protection Regulation
BCT	On-Board Computer Taxi
BOA	Special Investigator
CSN	Citizen Service Number
CA	Certification Authority
CI	Certification Body
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
GBA	Municipal Database
HSM	Hardware Security Module
ILT	Human Environment and Transport Inspectorate
NetSec	Network Security Controls
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Personal Unlocking Key
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Request for Comments
SLA	Service Level Agreement
TSP	Trust Service Provider, or Certification Service Provider
VOG	Certificate of Conduct
Wid	Compulsory Identification Act