



PKI Disclosure Statement (PDS)

Certification Authority BCT

Version 2.3

Date	July 12, 2019
Status	Final

Contents

	Contents—2
1	Introduction—3
2	Revision of this document—3
3	Contact Information—4
4	Certificate types, validation procedures and certificate usage—4
5	Limitations of Reliability—5
6	Obligations of Subscribers and Certificate Holders—5
7	Obligations of Trusted Parties regarding the check of certificate status—5
8	Limitation of Liability—5
9	Applicable Terms and Issuance Policy—6
10	Privacy Policy—6
11	Refund Policy—6
12	Applicable law, complaint and dispute resolution—6
13	CA and electronic storage licenses, trust marks and audit—6

1 Introduction

The (CA) Certificate Authority BCT issues smart cards for use with the On board Computer Taxi (BCT). These smart cards include digital certificates. The issuance of these certificates by the Certification Authority BCT is made under the Trust Service Provider (TSP) infrastructure of the Ministry of Infrastructure and Water Management.

This TSP is part of the PKIoverheid system.

The Certification Authority BCT has outsourced the actual issuance of cards and certificates to Kiwa Register B.V. and its subcontractors.

The purpose of this document is to summarize the main points of the:

- Uitgiftebeleid Boordcomputerkaarten en Systeemkaarten (Certificate Practice Statement, CPS); As soon as the CA BCT starts issuing PKIoverheid G3 certificates two versions of the CPS will be published: one (discontinued) version applicable to the G2 certificates and one current version applicable to the G3 certificates. Each end certificate contains a link to the applicable CPS.
- Algemene Voorwaarden PKIoverheid Certificaten, Dossierhouder BCT (Terms and Conditions PKIoverheid Certificates, Certification Authority BCT) and
- Ministeriële Regeling Gebruik Boordcomputer en Boordcomputerkaarten (Ministerial Regulation Use On Board Computer and On Board Computer Cards).

This document is not intended to replace the above-mentioned documents, and no rights can be derived from this document. For the full text of these documents reference is made to the electronic storage of the Certification Authority BCT, to be consulted at <https://bct.tsp.minienw.nl>

The definitions of the terms used in this document are included in the document Certificate Practice Statement.

2 Revision of this document

Version	Date	Summary changes
1.0	19-08-2011	Definitief vastgesteld
2.0	22-06-2017	Vertaling naar Engels
2.1	6-11-2017	ETSI TS 101 456" and with that complies with the requirements imposed on Certification Service Providers in the Wet elektronische handtekeningen (Weh) (Electronic Signatures Act). <i>replaced in:</i> ETSI EN 319 411-1 and ETSI EN 319 411-2" and with that complies with the requirements imposed on Certification Service Providers in the eIDAS verordening (electronic identification and trust services for electronic transactions in the internal market)

Version	Date	Summary changes
2.2	25-01-2018	<p>CWA 14169 <i>Replaced in</i> NEN-EN 419211</p> <p>BSI Management Systems BV <i>Replaced in</i> BSI Group The Netherlands</p> <p>The Certification Authority BCT is subject to a certification audit every three years. <i>Replaced in</i> The Certification Authority BCT is subject to a certification audit every two years.</p>
2.3	21-06-2019	<p>Changes:</p> <ul style="list-style-type: none"> - Name changed into Ministerie van Verkeer en Waterstaat / Ministry of Infrastructure and Water Management (also in logo) - Certificate Service Provider (CSP) changed into Trust Service Provider (TSP) - Removed Personal Confidentiality Certificate, not used in BCT - SSCD changed into QSCD - Wet bescherming persoonsgegevens changed into Algemene verordening gegevensbescherming (GDPR) - Updated link to TSP web-site - Alignment of Subscriber and Certificate Holder Obligations with Terms and Conditions

3 Contact Information

Human Environment and Transport Inspectorate
 Attn. Certification Authority BCT
 PO Box 16191
 2500 BD Den Haag

<https://bct.tsp.minienw.nl>

4 Certificate types, validation procedures and certificate usage

The Certification Authority issues the following types of certificates:

1. **Persoonsgebonden Authenticiteitcertificaat** (Personal Authenticity Certificate) - Used to authenticate the certificate holder;
2. **Persoonsgebonden Handtekeningcertificaat** (Personal Signature Certificate) - Used to verify an Electronic Signature;
3. **Services Certificaat (authenticiteit)** (Services Certificate (authenticity)) - Used for authentication of the organization of the Subscriber;
4. **Autonoom Apparaat Certificaat (authenticiteit)** (Autonomous Device Certificate (authenticity)) - Used for authentication of On board computer Taxi.

The Certification Authority BCT ensures a thorough determination of the information contained in the certificate. The data submitted by the applicant are verified using trusted sources.

5 Limitations of Reliability

The Certification Authority BCT does not limit the reliability of the certificates it issues. Under Chapter 8 you will find the limitation of liability.

6 Obligations of Subscribers and Certificate Holders

It is the responsibility of the Subscriber and Certificate Holder to ensure that:

- the information provided for the creation, issuance and withdrawal of a Certificate is correct;
- the Certificate is used solely for the On Board Computer Taxi;
- only they can access the private key related with the Certificate and the accompanying activation data;
- the activation data is stored safely and separately from the QSCD containing the private key;
- the Certification Authority will be notified immediately if:
 - the Private Key has been stolen, lost or otherwise has been compromised;
 - she suspects or could have suspected that the Qualified Signature Creation Device (QSCD), the activation data of the QSCD and / or other activation data have come or may have come in the hands of unauthorized persons;
 - inaccuracies in the Certificate are found;
 - the Private Key of the Certification Authority BCT, the IenW TSP and / or the Kingdom of the Netherlands has been stolen, lost or otherwise compromised.

7 Obligations of Trusted Parties regarding the check of certificate status

The Trusted Party is, on a case-by-case basis, required to independently determine that it is justified to trust the certificate. This she does by:

- determining the status of the Certificate based on the current Certificate Revocation List (CRL);
- verifying the authenticity of the information on the CRL by electronic signature with which the information is signed and the corresponding certification path;
- determining that the entire hierarchy in which the Certificate has been issued is valid. For System Cards also see the Letter to Parliament concerning new cards On Board Computer Taxi dated July 3rd 2019¹;
- taking all other precautionary measures which can be reasonably taken by trusted parties.

8 Limitation of Liability

The liability of the Certification Authority BCT is limited to the correct application of the Issuance Policy Procedures and the obligations under the General Terms and Conditions.

Damage caused by an error in a transaction based on a digital certificate is not covered by the liability.

¹ <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/03/nieuwe-kaarten-boordcomputer-taxi-bct>

9 Applicable Terms and Issuance Policy

The conditions under which the On board Computer Cards and System Cards are requested, issued and used are included in the following documents:

- Uitgiftebeleid Boordcomputerkaarten en Systeemkaarten (Issuance policy On board computer cards and system cards);
- Algemene Voorwaarden PKIoverheid Certificaten Dossierhouder BCT (General Terms and Conditions PKIoverheid Certificates Certification Authority BCT);
- Regeling gebruik boordcomputer en boordcomputerkaarten (Regulation for use On board computer and On board computer cards).

These documents can be retrieved via the electronic storage of the Certification Authority BCT, to be consulted at <https://bct.tsp.minienw.nl>

10 Privacy Policy

The processing of personal data by the Certification Authority BCT is done in accordance with the applicable regulations, in particular the Algemene Verordening Gegevensbescherming (General Data Protection Regulation). The data included in the Certificate is considered public information. However, the Certificate will not be made publicly available.

11 Refund Policy

Not applicable.

12 Applicable law, complaint and dispute resolution

The services of the Certification Authority BCT are governed by Dutch law.

Any dispute arising from this service or related thereto will initially be resolved between parties, if necessary with the help of intermediaries. If the dispute is not resolved, it will be submitted exclusively to the competent court at 's-Gravenhage.

13 CA and electronic storage licenses, trust marks and audit

The Certification Authority uses systems that are certified as Trustworthy System in accordance with the Technical Specification CEN TS 419261.

The TSP of the Ministry of Infrastructure and Water Management, including the Certification Authority BCT, is certified by BSI Group The Netherlands against the "Scheme for Certification of Certification Authorities against ETSI EN 319 411-1 and ETSI EN 319 411-2" and with that complies with the requirements imposed on Certification Service Providers in the eIDAS verordening (electronic identification and trust services for electronic transactions in the internal market).

Both the MinlenW TSP and the Certification Authority BCT also comply with the relevant parts of the Programma van Eisen van de PKIoverheid (PKIoverheid Requirements Program). This is demonstrable by using an audit statement issued by BSI Group The Netherlands.

The Certification Authority BCT is subject to a certification audit every two years. In the interim year a control audit is carried out.