ONLINE TRANSPORT INFORMATION

This Appendix 10 is applicable if and as far as *GTS* has granted **shipper** a non-transferable right of access to and use of the *online transport information*, as described in Chapter 1 of this Appendix. Access to and use of *B2B* is only permitted by means of a certificate, as described in the *certificate practice statement* (Chapter 2 of this Appendix) and access to and use of *Gasport* is only permitted by means of *MFA* as described in the *MFA practice statement* (Chapter 3 of this Appendix).

Chapter 1: Access to and use of the online transport information

1. Definitions

In addition to the definitions in the *general conditions*, for the purpose of this Appendix 10, except where the context expressly provides otherwise, the following terms shall have the meaning ascribed thereto below.

"B2B":
'Business-to-Business'; the application **shipper** can use to download transport information (with regard to measuring, allocating and balancing); the information to be downloaded is for **shipper**'s own use; a more detailed description of these *online transport information* can be found on the *website*;

"certificate practice statement" or *"CPS"*:
contains the procedure which *GTS* and co-operator N.V. Nederlandse Gasunie use to manage certificates;

"Gasport":
the application **shipper** can use to consult transport information (e.g. company information and information with regard to contracting, balancing, allocating, exposure and invoicing); the information is visible on-screen; a more detailed description of these *online transport information* can be found on the *website*;

"MFA practice statement" or *"MPS"*:
contains the procedure which *GTS* uses to manage access to *Gasport* via *Multi-Factor Authentication*;

"Multi-Factor Authentication" or *"MFA"*:
a platform through which access to *Gasport* is possible;

"online transport information":
the downloading or consulting of transport information via *Gasport* and/or *B2B* (from/on the *website*).

2. Online transport information

1. Use of the *online transport information* can start as soon as **shipper** has been certificated by *GTS* for access to the *online transport information* in accordance with the *CPS* or has been granted access by means of *MFA* in accordance with the *MPS*.

2. For certification, access via *MFA* and use of the *online transport information*, documentation is available in the form of handbooks and/or "online help" in the applications themselves. The Customerdesk will be available to answer operational and technical questions relating to the use of the applications (see Article 4).

3. **Shipper** declares that he will use the *online transport information* prudently. **Shipper** will in any event comply with the following rules:
   a. **Shipper** will not download near real-time transport information (information concerning the previous 36 hours) via *B2B* more frequently than this information is updated (the update frequency is stated in the handbook);

b. **Shipper** will not repeatedly download historic transport information (information that is more than 36 hours old) via *B2B*;

c. **Shipper** will store any transport information he has downloaded via *B2B* so he does not have to download the same transport information via *B2B* repeatedly.

GTS can call **shipper** to account if *GTS* believes that **shipper** is endangering the correct operation of the *online transport information*.

4. *GTS* makes a reasonable effort to ensure the timely and accurate availability of the *online transport information*, so that **shipper** will, with the help of this *online transport information*, be able to determine and adjust his own balance position. Although the utmost care has been taken to preserve the accuracy of the content of the *online transport information*, *GTS* cannot guarantee the absence of errors or incompleteness therein, or the transfer thereof.

5. For the benefit of analyses, to enable *GTS* to optimally deploy its *online transport information*, *GTS* may (ask another party to) register data concerning the use of the *online transport information* by **shipper**. *GTS* will treat all such information confidential.

3. Intellectual property

1. All copyright and any other rights to intellectual or industrial property and any similar rights, including related rights, database rights and rights to the protection of confidential commercial information relating to the *online transport information* will belong exclusively to *GTS* or its licensors. **Shipper** acknowledges these rights and will refrain from all forms of direct or indirect infringement of those rights. All documents provided by *GTS* via the *online transport information*, among which recommendations, reports, software, applications, etc., are and shall remain the property of *GTS* or its licensors, and are intended exclusively for **shipper***'s* own use.

2. **Shipper** is prohibited from publicising (which also means making available to third parties) all or part of any information obtained via the *online transport information* (expressly including information relating to the APX-ENDEX Within-Day Market) and/or to copy it in any form, including selling, altering/processing, making it available or distributing it, unless *GTS* has authorised such publication and/or copying in writing and/or it is based on legislation or a judicial ruling.

3. If **shipper** notices that third parties infringe the rights referred to in this article, **shipper** is obliged to notify *GTS* immediately in writing and, if *GTS* decides to take (legal) action against this infringement, to render *GTS* all assistance it may ask for, if necessary with the reimbursement of costs incurred.

4. Access to and use of online transport information

B2B

1. Access to *B2B* is based on digital certificates, as described in the *CPS*. Certificates are company-based.

2. **Shipper** will nominate one or more certificate holder(s), as described in the *CPS*, who are authorised to use the certificate. **Shipper** will notify *GTS* of the name, company name, address, email address and telephone number of the certificate holder. **Shipper** guarantees that the certificate will only be used by the certificate holder(s) he has authorised.

Gasport

3. Access to *Gasport* is only permitted by means of *MFA*, as described in the *MPS*. Access to *Gasport* is individual-based.

4. **Shipper** will nominate one or more employees, as described in the *MPS*, who are authorised to use *Gasport*. **Shipper** will notify *GTS* of the name, company name, address, email address and telephone number of the employees who are authorised to use *Gasport*. **Shipper** guarantees that *Gasport* will only be used by the employees he has authorised and will be responsible for a complete and correct list of employees having access to *Gasport*. **Shipper** will actively inform *GTS* with regard to any changes in this list of employees.

<u>General</u>

5. Communication regarding certification, access via *MFA* and the related practice statements shall take place either by email or registered letter, unless provided otherwise.

    Contact details

    Customerdesk
    P.O. Box 19
    9700 MA Groningen
    The Netherlands
    Tel +31 50 521 3333
    Email: customerdesk@gastransport.nl

Chapter 2: Certificate practice statement (CPS)

1. Definitions

In addition to the definitions in the *general conditions*, for the purpose of this Appendix 10, Chapter 2, except where the context expressly provides otherwise, the following terms shall have the meaning ascribed thereto below.

"administration partner":
N.V. Nederlandse Gasunie.

"applicant":
the person applying for a *certificate* as well as the legal entity he represents.

"certificate":
a digital document that at least identifies the *CA* and *applicant*, contains *applicant's* public key, period of validity and a certificate serial number and is digitally signed by the CA.

"certificate holder":
the person appointed by the legal entity he represents as holder of the *certificate*, as well as the legal entity on behalf of whom this person holds the *certificate*.

"certification authority" or *"CA":*
a legal entity authorized to issue *certificates*. The *CA* is subordinate to the *PCA*. Regarding this *CPS*, KPN Telecom is the CA.

"certificate revocation list" or *"CRL":*
a periodically issued list of identified *certificates* that have been suspended or revoked prior to their expiration dates.

"digital signature":
a transformation of a message, in such a way that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the *private key* that corresponds to the signer's public key and whether the message has been altered since the transformation was made.

"local registration authority" or *"LRA":*
a legal entity approved by a *CA* to assist *applicants* in applying for *certificates*, to approve such applications, to revoke *certificates* or to suspend them. Regarding this *CPS*, the function of *LRA* is performed by the *administration partner* on behalf of *GTS*.

"primary certification authority" or *"PCA":*
a legal entity that establishes practices for all certification authorities and users within its domain. Regarding this *CPS*, VeriSign is the *PCA*.

"private key":
a mathematical key used to create *digital signature*s and, depending upon the algorithm, used to decrypt messages or files encrypted with the corresponding public key.

2. General

This *CPS* sets out the procedures employed by *GTS* and its *administration partner* in the administration of *certificates*. A *certificate* enables *certificate holder* to uniquely identify himself in an environment managed by *GTS*, which is only accessible to other *certificate holders*.

GTS is entitled to change the technical properties of the *certificates*. No rights may be derived from the issued *certificates* other than those described in this *CPS*.

3. Obligations of the local registration Authority

1. *Certificate* applications and applications for a revocation or for a *CRL* will be honoured or rejected within three business days from the date of receipt, save suspension due to maintenance or other reasonably necessary or unavoidable interruptions, such as interruptions of the internet or malfunction of the back end system of the *PCA*.

2. When the *certificate* application has been honoured, *applicant* will be notified to the official address stated in the *certificate* application. The *LRA's* public key will be published on the website: https://certificaten.gastransportservices.nl. Issued *certificates* will not be published. Issued *certificates* are valid for one year after the date of issuance.

3. *Certificate holder* is granted a non-exclusive, non-transferable and personal right to use the *certificate* under the provisions set forth in this Appendix 10.

4. The *LRA* shall only be liable for direct damage to the extend such damage is caused by its wilful misconduct or gross negligence, which means an intentional or (consciously) reckless disregard of any obligation regarding the *CPS*. This limited liability is also stipulated on behalf of the *administration partner*. Security of the *LRA* system and related procedures are the responsibility of the *CA* and *PCA*.

4. Obligations of applicant and certificate holder

1. To apply for a *certificate*, *applicant* must correctly complete the application form. This form is available at the *website*. *Certificate holder* must be employed by the legal entity which he represents. *Applicant* warrants that the information issued in the *certificate* application is complete, actual and correct.

2. *Applicant* and *certificate holder* shall at their own expense and risk purchase the required hardware, software and licences for the use of the *certificate*. The *certificate* needs to be activated by the *applicant* within the period mentioned by the *LRA*; if not, the *certificate* will expire.

3. *Certificate holder* may only apply for a new *certificate* if the old *certificate* has been revoked or if the remaining period of validity is less than one month. An application to renew a *certificate* must take place at least a month before its expiration.

4. *Certificate holder* shall protect the secret elements associated with the *certificate* against compromise or disclosure. *Certificate holder* shall secure the *certificate* and the *private key* with appropriate measures. The *private keys* may only be decrypted by *certificate holder*. *Certificate holder* is advised to make copies of his *private keys*; he shall treat and protect these copies as if they were originals.

5. In the event of (possible) danger of the *private key*, *certificate holder* shall notify the *LRA* immediately. *Certificate holder* shall notify the *LRA* immediately if he discovers or suspects that a key for another *certificate* has been compromised.

6. *Certificate holder* warrants that the *certificate* and the *private key* are only used for the following applications: http security (TLS), email security, secure tunnels, code signing, message encryption and time stamping.

7. *Certificate holder* shall hold harmless and indemnify the *LRA* for any claim relating to the (contents of the) *certificate*, *private key* and *digital signature*.

5. Relying parties

1. The content of the *certificate* may only be relied upon by the following legal entities:
   - *PCA*, the *CA* or the *LRA*;
   - *administration partner* working on behalf of *GTS*;
   - legal entities certificated by the *LRA*.

2. Those relying on the *certificate* must confirm the validity of the *certificate* before using it, by checking the *CRL*. These parties must also verify the authenticity and integrity of the *CRL*. It is the *CA's* responsibility that the integrity of the *CRL* can be verified.

6. Confidentiality

1. Among other things, the following information will be considered as confidential information and treated accordingly:
   - Administrative data relating to *certificate holder* which are not included in a *certificate*;
   - Reasons for revoking a *certificate*;
   - Cryptographic keys and passwords of the *LRA*, and
   - Results of event recording.

2. An auditor will have full access to confidential data of *certificate holder*, which will be duly treated as confidential.

3. *Applicant* and *certificate holder* endorse the processing and registration of personal data in the administration of the *CA* and the *LRA*, such as the *CRL*. They also endorse the provision of confidential information by the *CA* to the Primary CA. The *LRA* cannot be held liable for the handling of this information by the *CA* and the *PCA*.

7. Revocation

1. The *LRA* or *CA* shall revoke the *certificate* immediately, without being liable for any consequence related to such revocation, if:
   - the contents of the *certificate* are inaccurate or incomplete;
   - the *private key*, or the medium on which it is stored, has been compromised or this is reasonably suspected;
   - the *certificate* is used either unlawfully or wrongfully, or this is reasonably suspected;
   - *certificate holder* requests the *LRA* to do so;
   - *certificate holder* fails to comply with the provisions set forth in this Appendix 10;
   - there is sufficient evidence that the certificated legal entity has ceased to exist.

2. If the *LRA's private key* is compromised or this is reasonably suspected, or the hardware or software resources of the *GTS* system are corrupted beyond recovery, the *LRA's certificate* will be revoked.

3. Revocation of a *certificate* is applied for by submitting a request to that effect by email to the address referred to in Article 4 of Chapter 1. The *LRA* will then contact *certificate holder* in person. When a *certificate* has been revoked, *certificate holder* will be notified by email to the address stated in the *certificate*. If the request is received during local business hours, it will be dealt with by the *LRA* immediately; if the request is received outside those hours, it will be dealt with on the next **business day**.

4. Revoked *certificates* will be published in a *CRL*, accessible to the relying parties stated in Article 6 of this Chapter 2. *Certificate holder* is no longer entitled to use the *certificate* or its digital keys once it has been revoked. Access to the *CRL* is exclusively via the relevant internet address stated in the *certificate*. The *CRL* will be updated by the *PCA*.

5. Revocation of a *certificate* does not impede *certificate holder's* obligations.

6. The *LRA* reserves the right to terminate his activities. The *LRA's certificate* will then be revoked. *Certificate holder* and the *CA* will be notified immediately by email.

Chapter 3: MFA practice statement (MPS)

1. Definitions

In addition to the definitions in the *general conditions*, for the purpose of this Appendix 10, Chapter 3, except where the context expressly provides otherwise, the following terms shall have the meaning ascribed thereto below.

"applicant":
the person applying for access to *Gasport* as well as the legal entity he represents.

"user":
the person appointed by the legal entity he represents as user of *Gasport*, as well as the legal entity on behalf of whom this person uses *Gasport*.

2. General

This *MPS* sets out the procedures employed by *GTS* in the administration of access to *Gasport* via *MFA*. Access via *MFA* enables users to uniquely identify themselves in an environment managed by *GTS*. User is granted a non-exclusive, non-transferable and personal right to access *Gasport* under the provisions set forth in this Appendix 10.

3. Obligations of applicant and user

1. To apply for access to *Gasport*, *applicant* must correctly complete the application form. This form is available at the *website*. *User* must be employed by the legal entity which he represents. *Applicant* warrants that the information issued in the application form is complete, actual and correct.

2. *Applicant* and *user* shall at their own expense and risk purchase the required hardware, software and licences for the use of *Gasport*.

3. *User* shall protect its password against compromise or disclosure. *User* shall secure the password with appropriate measures. The use of passwords by *user*, shall, with regards to security (e.g. length of passwords, content of passwords, period of change for passwords), need to comply with the procedures, as being published by *GTS*.

4. Revocation

1. GTS will revoke access to *Gasport* of a *user*, without being liable for any consequence related to such revocation, under the following conditions:
   - user shows no activity on Gasport during 180 consecutive days.
   - access is used either unlawfully or wrongfully, or this is reasonably suspected;
   - user asks GTS to do so;
   - user fails to comply with the provisions set forth in this Appendix 10;
   - there is sufficient evidence that the legal entity with access to Gasport has ceased to exist.

2. Revocation of access to *Gasport* of a *user* is applied for by submitting a request to that effect by email to the address referred to in Article 4 of Chapter 1.