

# EXHIBIT F

## 1 GENERAL

This Certificate Practice Statement (hereinafter: CPS) for *BBL Company* sets out the procedures employed by *BBL Company* and its administration partner N.V. Nederlandse Gasunie (hereinafter: Administration Partner) in the administration of Certificates. A Certificate enables a certificate holder to uniquely identify himself in an environment managed by *BBL Company*, which is only accessible to other certificate holders.

Communication regarding the CPS shall take place either by e-mail, fax or registered letter, unless provided otherwise.

### 1.1 Definitions

The definitions used in this CPS shall have the meaning as described in the Conditions. In addition and for the purpose of this CPS the following expressions shall have the meanings ascribed thereto below, except where the context expressly provides otherwise.

*"Applicant"*:

The person applying for a Certificate as well as the organization he represents;

*"Certificate"*:

A digital document that at least identifies the Certification Authority and Certificate Holder, contains Certificate Holder's public key, identifies the certificate's operational period, contains a certificate serial number and is digitally signed by the Certification Authority;

*"Certificate Holder"*:

The person appointed by the organization he represents as holder of the Certificate, as well as the organization on behalf of whom this person holds the Certificate;

*"Certification Authority"*:

An entity authorized to issue Certificates. The Certification Authority is subordinate to the Primary Certification Authority. Regarding this CPS, KPN Telecom is the Certification Authority;

*"Certificate Revocation List"*:

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"*:

An entity approved by a *Certification Authority* to assist *Applicants* in applying for *Certificates*, to approve such applications, to revoke *Certificates* or to suspend them. Regarding this CPS, the function of *Local Registration Authority* is performed by the *Administration Partner* on behalf of *BBL Company*;

*"Primary Certification Authority":*

An entity that establishes practices for all certification authorities and users within its domain. Regarding this CPS, VeriSign is the *Primary Certification Authority*;

*"Public Key":*

A mathematical key used as an encryption key that, combined with a *Private Key* derived from the *Public Key*, can be used to effectively encrypt messages and *Digital Signatures*;

*"Private Key":*

A mathematical key used to create *Digital Signatures* and, depending upon the algorithm, to decrypt messages or files encrypted with the corresponding *Public Key*.

## **1.2 Contact details**

BBL Company V.O.F.  
P.O. Box 225  
9700 AE Groningen  
The Netherlands  
Tel +31 50 521 3194  
Fax +31 50 521 3545  
Email: bbl-sales@bblcompany.com

## **2 GENERAL PROVISIONS**

### **2.1 Obligations of the *Local Registration Authority***

- 2.1.1 *Certificate* applications and applications for a revocation or for a *Certificate Revocation List* will be accepted 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 *Primary Certification Authority*.
- 2.1.2 When the *Certificate* application has been accepted, *Applicant* will be notified to the official address stated in the *Certificate* application. The *Local Registration Authority's Public Key* will be published on the official website of *BBL Company*. Issued *Certificates* will not be published. Issued *Certificates* are valid for one year after the date of issuance.
- 2.1.3 *Certificate Holder* is granted a non-exclusive, non-transferable and personal right to use the *Certificate* under the provisions set forth in this CPS, Exhibit E to the *Conditions* and the *Agreement*.
- 2.1.4 The *Local Registration Authority* shall exclusively be liable for direct damage 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 applicable to the *Administration Partner*. Security of the *Local Registration Authority* system and related procedures are the responsibility of the *Certification Authority* and *Primary Certification Authority*.

### **2.2 Obligations of *Applicant* and *Certificate Holder***

- 2.2.1 To apply for a *Certificate*, *Applicant* must correctly complete the application form. This form is available at the official website of *BBL Company*. *Certificate Holder* must be employed

within the area of responsibility of the organization which he represents. *Applicant* warrants the accuracy of the representations made in the *Certificate* application.

- 2.2.2 *Applicant* and *Certificate Holder* shall at their own expense and risk purchase the required hardware, software and licences for the use of the *Certificate*. A *Certificate* shall be activated by *Applicant* within the set term; if this has not been done, the *Certificate* shall expire.
- 2.2.3 *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 three months. An application to renew a *Certificate* must take place at least one month before its expiration.
- 2.2.4 *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 unlocked by *Certificate Holder*. *Certificate Holder* is advised to make copies of his *Private Keys* and he shall treat and protect them as if they were originals.
- 2.2.5 In the event of (possible) compromise of the *Private Key*, *Certificate Holder* shall notify the *Local Registration Authority* immediately. *Certificate Holder* shall notify the *Local Registration Authority* immediately if he discovers or suspects that a key for another *Certificate* has been compromised.
- 2.2.6 *Certificate Holder* warrants that the *Certificate* and the *Private Key* are only used for the following applications: http security (SSL/TLS), email security, secure tunnels, code signing, message encryption and time stamping.
- 2.2.7 *Certificate Holder* shall hold harmless and indemnify the *Local Registration Authority* for any claim relating to the (contents of the) *Certificate*, *Private Key* and *Digital Signature*.
- 2.3 Relying parties
- 2.3.1 The content of the *Certificate* may only be relied upon by the following entities:
- The *Primary Certification Authority*, the *Certification Authority* or the *Local Registration Authority*;
  - Administration partners working on behalf of *BBL Company*;
  - All organizations certificated by the *Local Registration Authority*.
- 2.3.2 Those relying on the *Certificate* must confirm the validity of the *Certificate* before using it, by checking the *Certificate Revocation List*. These parties must also verify the authenticity and integrity of the *Certificate Revocation List*. It is the *Certification Authority's* responsibility that the integrity of the *Certificate Revocation List* can be verified.

## 2.4 Confidentiality

2.4.1 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 *Local Registration Authority*;
- Results of event recording.

2.4.2 An auditor will have full access to confidential data of *Certificate Holder*, which will be duly treated as confidential.

2.4.3 *Applicant* and *Certificate Holder* endorse the processing and registration of personal data in the administration of the *Certification Authority* and the *Local Registration Authority*, such as the *Certificate Revocation List*. They also endorse the provision of confidential information by the *Certification Authority* to the *Primary Certification Authority*. The *Local Registration Authority* can not be held liable for the handling of this information by the *Certification Authority* and/or the *Primary Certification Authority*.

## 3 **CERTIFICATE REVOCATION**

3.1 The *Local Registration Authority* or *Certification Authority* 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 *Local Registration Authority* to do so;
- *Certificate Holder* fails to comply with this CPS, the Conditions or the *Agreement* ;
- there is sufficient evidence that the certificated entity has ceased to exist;
- the *Conditions* or the *Agreement* with *BBL Company* is terminated.

3.2 If the *Local Registration Authority's Private Key* is compromised or this is reasonably suspected, or the hardware or software resources of the *BBL Company* system are corrupted beyond recovery, the *Local Registration Authority's Certificate* will be revoked.

3.3 Revocation of a *Certificate* is applied for by submitting a request to that effect by email to the address referred to in Article 1.2. The *Local Registration Authority* 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 *Local Registration Authority* immediately; if the request is received outside those hours, it will be dealt with on the next business day.

3.4 Revoked *Certificates* will be published in a *Certificate Revocation List*, accessible to the relying parties stated in Article 2.3.1. *Certificate Holder* is no longer entitled to use the *Certificate* or its digital keys once it has been revoked. Access to the *Certificate Revocation List* is exclusively via the relevant internet address stated in the *Certificate*. The *Certificate Revocation List* will be updated by the *Primary Certification Authority*.

3.5 Revocation of a *Certificate* does not impede *Certificate Holder's* obligations under the *Conditions* or the *Agreement*.

- 3.6 The *Local Registration Authority* reserves the right to terminate the *Local Registration Authority's* activities. The *Local Registration Authority's Certificate* will then be revoked. *Certificate Holder* and the *Certification Authority* will be notified immediately by email.