Certipost General Conditions

Certipost digital certificates

Version	2.1
Effective date	03/05/2012
Document name	GTC_CTP_e-Certificates_V2_1.docx

1. Document control

Review history

Reviewer	Date	Action	Version	Status
CEPRAC members	15/11/2005	Initial version	1.0	Approved
CEPRAC members	15/08/2006	Logo change and new CA	1.2	Approved
CEPRAC members	14/12/2009	Rework policy overview table	1.3	Approved
CEPRAC members	12/01/2011	Minor changes and logo update	1.4	Approved
CEPRAC members	31/01/2012	Update for new PKI hierarchy and document refactoring	2.0	Approved
CEPRAC members	03/05/2012	Minor typographic changes	2.1	Approved

2. Index

1. DOCUMENT CONTROL 2
2. INDEX 3
3. DEFINITIONS AND ACRONYMS 4
4. PURPOSE 4
4.1. Services 4
4.2. Scope of the document 5
5. CERTIFICATE LIFE CYCLE 5
5.1. Certificate Request 5
5.2. Issuing and acceptance of a Certificate 5
5.3. Certificate Installation 6
5.4. Application and term of validity of the Certificate 6
5.5. Certificate renewal 6
6. USER AND DEVICE LIFE CYCLES 6
6.1. Users in "Certipost Token Manager" 6
6.2. Devices 6
7. RIGHTS AND OBLIGATIONS OF THE SUBSCRIBER AND THE CERTIFICATE HOLDER 7
8. RIGHTS AND OBLIGATIONS OF THE CERTIFICATE AUTHORITY AND THE CERTIFICATE SERVICE PROVIDER 9
9. RIGHTS AND OBLIGATIONS OF THE RELYING PARTY 9
10. BUSINESS AND LEGAL 10
10.1. Term and termination 10
10.2. Representations and guarantees 10
10.3. Liability limitation 11
10.4. Force Majeure 11
10.5. Technical problems and complaints 12
10.6. Protection of privacy 12
10.7. Confidentiality 12
10.8. Individual notices and communications with participants 12
10.9. Entire agreement 13
10.10. Amendments 13
10.11. Severability 13
10.12. Assignment 13
10.13. Dispute resolution provisions 14
10.14. Enforcement (attorneys' fees) 14
10.15. Governing law 14

3. Definitions and Acronyms

A generic document with the definitions and acronyms is available on-line on www.certipost.com. The modification of that document is subject to article 10.5 of the present General Conditions.

(Reference to RFC 3647: 1.6)

4. Purpose

4.1. Services

Certipost n.v./s.a. ("Certipost"), through its Certipost Certificate Services, and hereinafter also referred to as the "Certificate Authority" (CA), makes it possible to check the electronic identity of an end-entity, whether physical person, legal person, (web) server, device, address or object signing entity of the Customer, hereinafter referred to as the "Subject", using an asymmetric cryptographic technique.

- If the Subject is a physical person who belongs to a Customer's legal person organization, then this organization is called the Subscriber.
- If the Subject is a physical person who does not belong to a legal person organization but acts as an individual Customer, then this Subject is also called the Subscriber.
- If the Subject is another end-entity, such as a legal person organization or a server, the Subject belongs to a Customer's legal person organization which is called the Subscriber. There may be one or more physical persons ("Mandated Certificate Holders") who will act on behalf of the Subject for the request, the approval, the renewal and the revocation of Certificates.

The Customer equals the Subscriber and always has overall responsibility for the Subject and Mandated Certificate Holders, if any.

To this end, the CA issues a Certificate that, according to the Certificate type and as identified by the Certificate Policy (CP), provides a certain level of assurance of the correctness of authentication of the Customer (called the Subscriber), based on the registration process, and of the link between the end-entity's identity (called the Subject), its optional attributes and the Certificate's Public Key.

The Certificate is issued under a Certificate Policy (CP), i.e. a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. One or more Certificate Policy Documents are used per Certificate Type as referred to by unique reference numbers (OIDs). The CP specifies which conformance declarations are made for the particular Certificate Type and which other requirements exist (e.g. the appropriate Certificate usage, the place and method of key pair generation, the cryptographic parameters etc.). The way the CP is realized is described in the Certificate Practice Statement (CPS).

This CP OID can be used by third parties to determine the applicability and trustworthiness of a Certificate for a particular application.

Certipost n.v./s.a., is also a "Certificate Service Provider" (CSP), which can provide the following services:

- Registration service: verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the Certificate generation service.
- Certificate generation service: creates and signs Certificates based on the identity and other attributes verified by the registration service.
- Distribution service: distributes Certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

- Revocation status service: provides Certificate revocation status information to relying parties. This may be based upon Certificate revocation lists or a real time service which provides status information on an individual basis. The status information may be updated on a regular basis and hence may not reflect the current status of the Certificate.
- Subject device provision service: prepares and provides a private key holding device to Subjects.

4.2. Scope of the document

This document specifies the General Conditions of using the services provided by the CA and CSP "Certipost". It should give the "Subject" and "Subscriber" an understanding of the Certificate, user and (user) device life cycles and the main rights and obligations of the different parties. The more extended description can be found in the CPS.

The present General Conditions can be supplemented by additional Subscriber Agreements which then take precedence over the General Conditions.

As a result, the Agreement between Certipost and the Customer consists of the Order Form (if any) the delivery receipt (if any), the Subscriber Agreement (if any), the present General Conditions, the CP and the CPS.

5. Certificate life cycle

5.1. Certificate Request

The Subscriber can acquire a Certificate:

- either online via the webshop of Certipost on http://www.certipost.be/webshop
- or by means stipulated in the Subscriber Agreement, if any.

By requesting a Certificate the Subscriber and – if applicable – the Subject or Mandated Certificate Holder accept the present General Conditions, the related CP and the CPS, as available on-line at the following Internet address: http://pki.certipost.com.

The Subscriber likewise acknowledges having knowledge of these documents, which, together with the Order Form, are an integral part of the Agreement between the Customer and Certipost.

The Subscriber and – if applicable – the Subject or Mandated Certificate Holder shall strictly follow the required procedure to request a Certificate as fully described in the related purchase order.

5.2. Issuing and acceptance of a Certificate

Acceptance of the application for a Certificate by the CA shall be subject to verification by a Registration Authority:

- of the data on the Certificate Request;
- of the additional data provided in the other documents requested by Certipost;
- the matching between these data;
- in case the Subscriber has generated a private/public key pair, whether the Subscriber is in possession of the private key that has been used to sign the Certificate Request (this consists of the public key and the personal and professional data); the Key Pair comprises the Private Key and the Public Key.

The provisions with regard to the Registration Authority are defined in the CP.

Once this verification is done, the CA will continue with either the issuance of the Certificate in case the Subscriber has generated his private/public key pair, or either, will proceed to the generation of the private/public key pair and issue the related Certificate in accordance with the requirements as provided in the related CP and in the CPS.

The period of time cited for a Certificate to be issued is purely indicative and does not give rise to entitlement to any possible compensation. Should the CA fail to meet this deadline, it will inform the Subscriber thereof and set a new deadline, it will make every endeavor to comply with.

5.3. Certificate Installation

The Customer shall have personal and sole responsibility for the installation of the Certificate.

5.4. Application and term of validity of the Certificate

The Certificate is valid for a fixed term as selected by the Subscriber according to the related Order Form and CP. This time may be shortened by a Subscriber or a Mandated Certificate Holder. The Certificate may be renewable depending on the CP and subject to the conditions in the CP. On expiry, and if not renewed, the Subscriber may apply for a new Certificate, in accordance with section 5.1 of these General Conditions.

5.5. Certificate renewal

Any Subscriber or – if applicable – the Subject or Mandated Certificate Holder wishing to renew a Certificate in the case this is allowed by the CP and the conditions for renewal are met, must request this renewal from the CA, which will take suitable measures.

Without prejudice to clause 10.1, the Agreement for a certain Certificate terminates ipso jure, without entitlement to damages and interest, on the day on which the concerned Certificate expires. The Customer may then apply for a new Certificate, in accordance with section 5.1 of these General Conditions.

6. User and device life cycles

6.1. Users in "Certipost Token Manager"

A Subscriber may delegate different tasks in relation with the Certificate life cycle and the Subscriber's rights and obligations to either:

- physical person Subjects who belong to the Subscriber's legal person organization
- Mandated Certificate Holders who act on behalf of the Subscriber

As far as the related Order Form and/or Subscriber Agreement confirms parties' agreement therefore, the above entities can be regarded as users of Certipost Token Manager. Certipost Token Manager is a cloud-based web application that enables Subscribers and their physical person Subjects to manage their own Certificates and private key holding devices (also called tokens).

By accepting these General Conditions, the Subscribers, their physical person Subjects and their Mandated Certificate Holders accept to be duly identified and authenticated by the CA and provisioned when using the Certipost delegation and self-servicing applications. These users accept to make use of these Certipost applications according to the defined conditions which includes the right of the CA to register, maintain, store and archive user data for as long as stipulated in the retention period specified in the CP.

Notwithstanding anything else mentioned in the Agreement, the CA however has no obligation to always provide a service for delegated and self-service management of Certificates and private key holding devices.

6.2. Devices

In case the Subscriber makes use of private key holding devices in accordance with the CP, the acceptance of the General Conditions also implies the acceptance of making use of those private key holding devices provided by the "Subject device provision service" which is defined in the Order Form or the CP. The rights and obligations concerning these devices and the Subject device provision service are to be considered an integral part of the General Conditions.

7. Rights and obligations of the Subscriber and the Certificate Holder

The Subscriber hereby acknowledges having knowledge of and explicitly accepting the CPS and related CPs for the desired Certificate, for which the object identification numbers are recorded in the application.

The Subscriber must comply rigorously with these General Conditions and with the CPS and CP.

If the Subject and Subscriber are separate entities, the Subscriber shall make the Subject aware of those obligations applicable to the Subject.

The specific rights and obligations are:

- The Key Pair generation must be undertaken in accordance with the CP. If the Subscriber or Subject generates the Subject's keys, the Subscriber is obliged to generate the subject's keys using an algorithm and a key length recognized as being fit for the purposes of the CP.
- The Subscriber must ensure that at the time a Certificate request is made there is no outstanding Certificate whatsoever for its Public Key (whether issued by this CA or another certification authority) nor is there any other application for a Certificate (filed with this CA or another certification authority) in this regard.
- The Subscriber must ensure that no further Certificate application will be made (to this CA or another certification authority) for a Certificate for the same Public Key unless the application is related to a renewal or re-certification of an existing Certificate and the situations and CP allow this.
- The Subscriber must submit precise, accurate and complete information to the CA in accordance with the requirements of this policy, particularly with regards to registration. The Subscriber is responsible for the accuracy of the data provided to the CA.
- The physical person Subjects or Mandated Certificate Holders must verify the accuracy and completeness of the Certificate data when queried by the Certipost delegation and self-servicing applications during the issuance process and, in case of any deviations, to not accept the Certificate issuance. Thus, once the Certificate has been issued it is deemed to have been accepted and there is no recourse available to the Subscriber in the event that the Certificate is inaccurate or incomplete. If this should occur the Subscriber is obliged to revoke the Certificate and acquire a new one.
- In case the Subscriber is not entitled to make use of the Certipost delegation and self-servicing applications, the Certificate is deemed to have been accepted by the Subscriber on the eighth day after its publication in the Public Directory of Certificates specified in the CPS or when it is first used by the Subscriber, whichever occurs first, except if otherwise described in the CP. During this intervening period, the Subscriber is responsible for verifying the accuracy of the published Certificate’s content. The Subscriber must notify the CA without delay of any inconsistency noted between the information in the Agreement and the content of the Certificate. The CA must then revoke the Certificate and take the necessary measures to re-issue it. This is the sole recourse available to the Subscriber in the event that the Certificate is not accepted.
- The Subscriber hereby explicitly authorizes the CA to publish the Certificate, once it has been issued, in the Public Directory specified in the CPS, except if otherwise described in the CP. The Subscriber and Subject likewise accept that any third party can freely consult this Directory and obtain a copy of the Certificate.
- The Subscriber hereby agrees to the retention by the CA, for a period after expiry of the last Certificate pursuant to this registration as specified in the CP’s retention period, of all information used for the purposes of:
    - registration
    - provisioning users in the Certipost delegation and self-servicing applications
    - provisioning of any private key holding device (including SSCD if this applies)
    - suspension or revocation of the Certificate

- In the event that the CA ceases its activities, the Subscriber shall permit the above information to be transmitted to third parties under the same or comparable terms and conditions as those applicable under this Agreement.
- The Subscriber shall have personal and sole liability for the confidentiality, integrity and use of the Subject Private Key. This means, inter alia, that the Subscriber must:
    - use reliable systems to protect the Private Key at all times
    - take the necessary measures to prevent the loss, disclosure, alteration or unauthorized use of the Private Key.
- In using the Key Pair, the Subscriber must comply with any limitations indicated in the Certificate's CPs or any contractual agreement. In particular, the Subscriber must only use its Key Pair with the purpose indicated in the Certificate and CP.
- In case this is contractually allowed, the Subscriber is entitled to use the Certipost delegation and self-servicing applications to suspend or revoke the Certificate, or to reinstate a Certificate which has previously been suspended in case this is allowed. It is not possible to reverse the revocation of a Certificate. In case the Certipost delegation and self-servicing applications are not available, the Subscriber may contact the CA and make the following requests by using the form and procedure in Annex 1: (1) a Suspension request, (2) an Un-suspension request following Suspension, or (3) a Certificate Revocation request. These are annexed to the General Conditions.
- The Subscriber must suspend or revoke the Certificate or, if this is not possible due to the unavailability of the Certipost delegation and self-servicing applications, to notify the CA in order to suspend / revoke the Certificate without any reasonable delay by means specified in procedures described in Annex 1, if any of the following occur up to the end of the validity period indicated in the Certificate:
    - the Subject's Private Key has been lost (e.g. by forgetting the PIN number needed to use the Key), stolen, potentially compromised; or
    - control over the Subject's Private Key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
    - inaccuracy or changes to the Certificate content, as notified to the Subscriber or to the Subject or as soon as the Subscriber or Subject becomes aware of this by itself.
- The Subscriber must not unsuspend Certificates in case of the situation specified in the previous point.
- The Subscriber must inform the CA of any changes in information that is not included on the Certificate but was sent to the CA during the registration process.
- The Subscriber must, following compromise, immediately and permanently discontinue the use of the Subject's Private Key
- In the case of being informed that the CA which issued the Subjects' Certificate has been compromised, the Subscriber must ensure that the Certificate is no longer used by the Subjects.
- If allowed by the CP and supported by the Certificate Type:
    - The Subscriber is entitled to request the recovery of an archived Key by the physical person (Subject) in case of a personal Certificate for the duration of the archiving period specified in the CP. The CA is entitled to require the physical person and the Subscriber to be an active Customer of the CA. This may result in a reasonable fee to rejoin the service in case the former Subscriber and/or its Subject is no longer a Customer with a contractual agreement with the CA.
    - The Subscriber is entitled to request the recovery of an archived Key by a Mandated Certificate Holder belonging to a Subscriber's legal person organization which is still a Customer of the CA in the case of non-personal Certificates, for the duration of the archiving period specified in the CP.
- If allowed by the CP and supported by the Certificate Type: the Subscriber must accept Key recovery by a mandated person of Certipost in case a legal obligation exists to do so.

The following particular Subscriber obligations exist in case of specific CPs and/or Certificate usages:

- for the Certificates used in relation with Advanced Electronic Signatures:
  - the obligation to ensure that the Subject's Private Key can be maintained under the Subject's sole control
  - the obligation to only use the Key Pair for electronic signatures and in accordance with any other limitations notified to the Subscriber;
- if the Certificate policy requires use of an SSCD
  - the obligation to only use the Certificate with electronic signatures created using such a device
  - the obligation to generate the Subject's Keys within the particular SSCD to be used for signing.

8. Rights and obligations of the Certificate Authority and the Certificate Service Provider

The general obligations of the CA and the CSP are defined in the CPS.

In particular the CA has the following rights and obligations:

- The CA has the right to suspend or revoke the Certificate or reinstate it following suspension under the circumstances described in the CPS, the related CP and these General Conditions, subject to compliance with the terms, conditions and procedures specified in the CPS.
- The Registration Authority has the right to demand the suspension or revocation of the Certificate in the cases set out in the CPS and CP.
- On issue, the CA has the right to publish the Certificate in its Public Directory of Certificates, except if stated otherwise in the CP.
- If the Certificate is suspended or revoked, it must be listed (under its serial number) in the CA's CRL, together with the grounds therefore. If the Certificate is reinstated after suspension, all mention of the Certificate must be removed from the CRL.
- The CA will make every endeavor and take the necessary measures to ensure that the Public Register of the CA's Certificates and the CRL can be consulted by any person at any time.
- The CA can inform the Subscriber of the forthcoming expiry of the Certificate at a reasonable time before it expires. This notification can be issued, by default, by e-mail and can indicate, the date on which the Certificate will cease to be valid.

9. Rights and obligations of the relying party

Relying parties who want to make use of the Certificates issued in accordance with the related CP must:

- verify the cryptographic validity of the Certificate and the entire certification chain
- verify the validity of the Certificate by checking the following against the CA's Certificate Revocation Lists (CRLs) referred to in the CP
- take into account all restrictions on use of the Certificate specified in the Certificate itself, and the related CP
- take all the other precautions with regard to use of the Certificate set out in the related CP or elsewhere
- depending on the CP and certificate use, take into account a grace period for the revocation period which includes:
  - a grace period for the propagation delay (between the reporting of the revocation request and the actual availability of up-to-date revocation information for relying parties); in practice this will be the CRL issuance frequency;
  - a grace period for the delay in between a cause for revocation existed (e.g. the device holding the Private Key has been stolen) and the actual reporting; in practice it will not always be

possible for the Certificate holder or mandated person to make a report to the revocation service immediately;

- the relying party may choose to accept the risk of not applying a grace period either in general or for a first checking of validity for either of the above components; the CA is not responsible if the relying party suffers damages due to outdated validity data in the case the relying party chooses not to take a grace period into account for either initial checking or a later (re-)validation.

10. Business and legal

10.1. Term and termination

The Agreement shall enter into effect on the day on which the Order Form completed and signed by the Customer is accepted by Certipost.

In the event of a material breach of, or material failure to comply with, the Agreement by the Customer or by Certipost, the party not at fault shall serve notice on the other party by registered letter. If that other party fails to remedy such default within 30 calendar days of the date on which the registered letter is sent, the party not at fault may terminate the Agreement, without prejudice to the latter's right to be indemnified for its damages.

The Agreement shall end at bankruptcy of a party, without prejudice to the right of the other party to be indemnified for its damages.

The Agreement shall terminate ipso jure if the Certificate is revoked or expires, regardless of the grounds therefore. This may include a revocation imposed by an unforeseeable degradation of rigidity of a cryptographic algorithm. However, the same Agreement can be reactivated when the certificate is recertified and re-issued or has been renewed.

If the Customer however has a valid Subscriber Agreement or (Web Shop) Order Form that allows the Customer to continue using the Certipost delegation and self-servicing applications during a specified term for requesting new Certificates and/or other Certificate services, even if the original certificate has expired or has been revoked, then the Agreement is considered to govern all ordered Certipost Certificate services towards the Customer for the stipulated term and is not terminated at the revocation/expiry of a Certificate, unless a non-remedied default has occurred as specified above.

When the Agreement comes to an end, irrespective of the grounds therefore, the Subscriber must immediately cease all use whatsoever of the Certificate(s) and of the Certipost delegation and self-servicing applications (if any). If, on termination of the Agreement on any ground whatsoever, the term of validity of the Certificate(s) has not yet lapsed, the CA must revoke the Certificate(s) forthwith, without prior notice or compensation. The expiry or termination of the Agreement, irrespective of the grounds therefore, shall not prejudice any mutual rights and obligations of the parties thereto that are intended to extend beyond the term of the Agreement.

10.2. Representations and guarantees

The only guarantees offered by Certipost are those set out in the present General Conditions.

The CA shall solely guarantee:

- the accuracy of the data given in the Certificate on the date it is issued;
- rigorous compliance, at the time the Certificate is issued, with the relevant procedures specified in the CPS and related CP.

The CA does not guarantee:

- the accuracy of any unverifiable piece of information contained in Certificates, except as it may be stated in the relevant CP;

- the accuracy, authenticity, completeness or fitness of any information contained in free, test or demo Certificates.

The Customer shall hold Certipost and its agent(s) and contractors harmless in the event of any proceedings, claim or complaint, by one of the parties hereto or by any third party whatsoever, alleging damage or loss as a result of the use of, or confidence placed in, a Certificate, in the event that the Customer:

- does not provide Certipost with accurate data
- misleads Certipost (a.o. falsehood or misrepresentation of fact or concealment of a material fact by Customer)
- does not protect the Subscriber's Private Key in a trustworthy manner (in accordance with the state-of-the-art techniques and using reliable key protection systems).

The Certificate provides no guarantee that:

- data on which the Private Key is applied is free from malware, such as viruses, bugs, Trojan horses or logic bombs; the Customer has full liability for any such occurrence;
- use of data on which the Private Key is applied will not result, inter alia, in data loss or in damage to, for example, a software package or the operating systems of third-party users; the Customer has full liability for any such incidents;
- data on which the Private Key is applied will not be intercepted by third parties.

10.3. Liability limitation

Without prejudice to any other Certipost liability limitations possibly set forth in any applicable contractual document (e.g. a Subscriber Agreement), the following liability limitation applies to liability under contract, tort and any other form of liability claim, to the extent permitted by law:

a) In no event shall Certipost be liable for any indirect, immaterial or consequential damages or for any loss of profit or loss of data, arising from or in connection with the use, delivery, license, performance or non-performance of, or the reliance on, Certificates, electronic signatures or other transactions or services under the Agreement, even if Certipost has been advised of the possibility of such damages.

b) In no event shall Certipost be liable for any kind of damage arising from or in connection with the use, performance or non-performance of, or the reliance on, a suspended, revoked or expired Certificate or a free/test/demo Certificate or in case of fraud or wilful misconduct of a party other than Certipost.

c) The cumulated aggregate liability of Certipost towards any and all persons (including but not limited towards the Customer, Subscriber, applicants, recipients and relying parties), concerning a specific Certificate (including for the aggregate of all electronic signatures and transactions related to such Certificate), shall not exceed the applicable liability cap for such Certificate as set forth below:

- liability cap for Certificates with assurance level Qualified or Normalised: EUR 25,000
- liability cap for Certificates with assurance level Lightweight: EUR 250

Such liability cap per Certificate shall remain the same regardless of the number of electronic signatures, transactions or claims related to such Certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a competent jurisdiction. In no event shall Certipost be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

If and to the extent such limitations would not be permitted under applicable law, then the liability of Certipost shall be limited to the maximum extent permitted under applicable law.

10.4. Force Majeure

Neither party shall be liable for any delay or failure to perform the Agreement that is attributable to facts or circumstances which (i) can reasonably be deemed to be beyond the control of one of the parties; (ii) are

unforeseen and (iii) are unavoidable. Any party invoking such facts or circumstances must make every endeavor to prevent force majeure occurring and limit the duration thereof. It must immediately notify the other party in writing or equivalent should it occur and also inform the other party when these facts or circumstances come to an end.

10.5. Technical problems and complaints

In the event of technical problems with regard to the Certificate or complaints about the services provided under this Agreement, the Customer may contact the Helpdesk (Tel: +32(0)70 22 55 33; Fax: +32(0)70 22 55 01; e-mail: helpdesk@certipost.com).

10.6. Protection of privacy

In applying for a Certificate, personal data are communicated by the Customer.

Data communicated to the CA and the RA by the Customer is entered into the databases held by the CA and by the RA. This data must be used by the CA solely for the purposes of providing certification services (notably for issuing and managing Certificates). Additional information may be obtained from the public registry of the Commission for the Protection of Privacy, Hoogstraat 139, B-1000 Brussels.

Personal data communicated by the Customer to the CA will be incorporated into files held by Certipost, and, as appropriate, in files held by the RA. This data shall only be used for the purposes of providing Certipost services. The concerned natural persons have a right to access and amend their data. For this purpose the concerned person must send a signed and dated request together with a copy of his/her identity card to the Certipost Legal Department at the head office in Belgium.

The CPS specifies the provisions made to protect the privacy of this data.

10.7. Confidentiality

The parties must not disclose to any third party confidential data arising with respect to the conclusion, performance or expiry of the Agreement and must use any such data solely for the purposes of performance of the Agreement.

All data relating to the Subscriber, Certipost and the content of the Agreement shall be deemed by both parties to be confidential information. All confidential data disclosed by the parties belongs to and remains the property of the disclosing party.

This duty of confidentiality shall continue to apply throughout the term of the Agreement and for three years thereafter, irrespective of the grounds for termination.

10.8. Individual notices and communications with participants

To be valid, any communication between the Customer and Certipost must be sent to the addresses cited on the Order Form.

For communications requested for the registration process (e.g. copy identity card, mandate, …), the sender will use a signed letter or an e-mail signed with an electronic signature, with the exception of any notification of a change of address by either party which is to be communicated by registered letter, fax or e-mail with an electronic signature.

Subject to what is mentioned above, it is hereby agreed between the parties that communication may also be undertaken by validly signed e-mail. Unless explicitly indicated otherwise, the parties accept that all validly signed e-mail communications between them have the same legal status as written and signed correspondence except for making new contractual agreements or for litigation purposes.

Subject to proof to the contrary, information relating to any valid communication, the Agreement and payment records held by the CA or the RA on a lasting medium have probative force equivalent to that of original documents.

10.9. Entire agreement

The Agreement concluded between the Customer and Certipost comprises the Order Form (including the Certificate delivery receipt) (if any), possibly through the Certipost Webshop if accepted by Certipost, the Subscriber Agreement (if any), the present General Conditions and the related CP and CPS.

In the event of any conflict, the order of precedence shall be as follows:

- the Subscriber Agreement or accepted Web Shop Order Form (if applicable) has priority over the other documents;
- the Definitions and Acronyms have priority over the General Conditions, CP and CPS;
- the General Conditions have priority over the related CP and CPS; and,
- the related CP has priority over the CPS.

The rights and obligations of Certipost and the Customer shall be limited solely to those set out in the Agreement. This Agreement supersedes, replaces and renders null and void all prior and contemporaneous written or oral understandings, obligations, agreements, negotiations and proposals relating to the same subject matter.

Any conditions on any purchase order or other document whatsoever which GDF SUEZ issues in connection with the Agreement shall not be binding on Certipost nor be used to interpret the Agreement.

Any failure by Certipost or the Customer to exercise a right shall not, under any circumstances, be construed as abandonment thereof.

10.10. Amendments

Changes to these General Conditions are indicated by appropriate versioning.

Certipost reserves the right to change the provisions of these General Conditions. Certipost must inform the Customer thereof in advance through an announcement published on its webpage (http://www.certipost.be) or sent by e-mail. If the Customer rejects the changes, it shall have 14 calendar days, from the date on which the e-mail announcement is sent, in which to terminate the Agreement. If the Customer does not terminate the Agreement, it shall be deemed to have accepted the changes.

Changes to the CPS that will not materially reduce the assurance that a CP or its implementation provides, and that will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates, do not require a change in the CP OID or the CPS pointer (URL) in the Certificates. The CPS describes the rules and procedures for changing the CPS.

10.11. Severability

If any provision of this Agreement, including the liability limitation clause, is found to be invalid or unenforceable, the remainder of this Agreement is interpreted in such manner as to the effect the original intention of the parties.

In the event that one of the provisions of the Agreement is declared null and void or unenforceable, it shall be deemed not to have been written and all other clauses shall continue to have effect. The Customer and Certipost must make every effort to replace any provision declared null and void or unenforceable by a provision, the commercial intent of which is as close as possible to that which is void or unenforceable.

10.12. Assignment

Certipost may, at any time, transfer, and thereby discharge, in full or in part, its rights and obligations under this Agreement to a subsidiary or allied company, without the Customer's consent. Any transfer, in full or in part, by the Customer of its rights and obligations under the Agreement shall be subject to the prior written consent of Certipost.

10.13. Dispute resolution provisions

In the event of a conflict with respect to the validity, interpretation or performance of the Agreement, Certipost and the Customer must make every endeavor to achieve an amicable settlement. If an amicable settlement cannot be reached, the courts of Brussels shall have sole jurisdiction for any dispute relating to this Agreement.

Notwithstanding this last provision, when applicable, any claim relating to the suspension or revocation of the Certificate, or citing any such suspension or revocation, which contests grounds which are covered by the duty of professional secrecy on the part of the CA shall be subject to arbitration under the rules of the CEPANI (Belgian Center for the Study and Practice of National and International Arbitration).

10.14. Enforcement (attorneys' fees)

A party prevailing in any dispute arising out of this Agreement is not entitled to attorneys' fees as part of its recovery.

10.15. Governing law

This Agreement is governed by the Belgian law.

ANNEX 1

Certipost Certificate Suspension, Unsuspension and Revocation form

Last name of applicant: First name of the applicant:

Company

Street name and house number:

Postal Code City VAT number

Telephone Fax E-mail

hereby applies for ☐ Suspension ☐ Unsuspension following suspension ☐ Revocation
on the following ground(s) (insofar as these are not covered by professional secrecy):

of the certificate issued to:

Last name of the holder: First name(s) of the holder:

Organization:

Certificate serial number:

Contract number:

Suspension/revocation password:

The person applying therefore is:

- ☐ The holder of the Certificate
- ☐ A legal representative of the organization
- ☐ The duly appointed proxy of the organization's legal representative.
- ☐ Other (please specify):

Date: Signature:

Fill in and return this form by fax to **+32(0)70 22 55 01** or by post to Certipost Certification Services, Ninovesteenweg, 196, B-9320 Erembodegem (Aalst).

RA approval (Internal use Certipost)
Name: Date: Signature: