CPS DigiNotar 30 OCTOBER 2007

'CPS DigiNotar' 'CPS DigiNotar General'
OID (2.16.528.1.1001.1.1.1)

Version 3.5

30 October 2007

This version of the CPS replaces any and all previous versions.

Certificate type Public	Policy OID
Person-specific Organisation Certificate/Person-specific Company Certificate P#12 Smartcard USB	2.16.528.1.1001.1.1.1.2.4.1.2.2 2.16.528.1.1001.1.1.1.2.4.1.3.2 2.16.528.1.1001.1.1.1.2.4.1.4.2
Envelope Certificate	2.16.528.1.1001.1.1.1.5.4.1.2.2
Business Relation Certificate	2.16.528.1.1001.1.1.1.6.4.1.2.2
SSL Server Certificate	2.16.528.1.1001.1.1.1.7.6.1.1.1
SSL Server Certificate (P#12)	2.16.528.1.1001.1.1.1.7.6.1.2.2
Extended Validation SSL Certificate	2.16.528.1.1001.1.1.1.12.6.1.1.1
Signing Server Certificate (P#12)	2.16.528.1.1001.1.1.1.7.8.1.2.2
Software Signing Certificate (P#12)	2.16.528.1.1001.1.1.1.7.9.1.2.2

Table of Contents

1. Introduction

1.1 Civil-law notaries in the digital world: DigiNotar

People need security and reliability, both in the physical world and the digital world of the Internet. Traditionally, in the Netherlands, civil-law notaries provided for this need when agreements were set down on paper. Nowadays, they can ensure security and reliability in the electronic exchange or archiving of information. In this regard, the civil-law notary acts as a Trusted Third Party (TTP).

DigiNotar is the notarial profession's collaborative partnership for electronic services. DigiNotar offers notarial TTP services as a partnership organisation.

1.2 What is the CPS DigiNotar?

This document sets out the instructions and general terms and conditions for the Certification Authority activities of the DigiNotar organisation and is DigiNotar's Certificate Practice Statement (CPS). The document forms a part of the contractual agreements over the provision of DigiNotar Certificate Services and contains a description of the parties' rights and obligations in connection with the use of these services. The document also aims to offer insight into the involvement of the notarial profession in the provision of DigiNotar Certificate Services and the significance of this involvement.

The CPS DigiNotar is subject to change and will be adapted periodically. Additional documents will also be published for other services to be provided from the DigiNotar partnership.

1.3 Maintenance, questions, comments

The CPS DigiNotar has been drawn up and is maintained by:

DigiNotar B.V.
Vondellaan 8
1942 LJ Beverwijk, the Netherlands
Tel: +31(0)251 - 268888
Fax: +31(0)251 - 268800
E-mail: Info@diginotar.nl
WWW: http://www.diginotar.nl

This document shall be cited as 'CPS DigiNotar' and 'CPS DigiNotar General – signature without qualification'. It is intended for interested parties who use or rely on the DigiNotar Certificates. The CPS DigiNotar can be obtained from the DigiNotar website (see the above e-mail address) and in paper form from the above street address. Postage and handling costs will be charged if a paper copy of this document is requested.

We welcome comments about the content of the CPS DigiNotar. You can use one of the addresses above for this purpose.

2. Definitions

2.1 Certificate

An electronic document that meets the technical specifications (as included in the Technical Specifications Appendix) and offers guarantees with respect to the identity of the Client and/or the User and can offer guarantees with regard to this party's authority to electronically exchange messages and other forms of data communication using a Key Pair consisting of a Private key and a Public key.

2.2 Certificate Practice Statement (CPS)

Instructions and general terms and conditions for the acquisition and use of DigiNotar Certificate Services. The Certificate Practice Statement is referred to in this document as: the CPS.

2.3 Certification Authority (CA)

A trusted authority which creates and grants Certificates. Within the DigiNotar model, DigiNotar B.V. is the Certificate Authority. The Certificate Authority is referred to in this CPS as: the CA.

2.4 Client

The natural person or legal person which whom DigiNotar or a DigiNotar TTP civil-law notary has concluded an agreement for the provision of DigiNotar Certificate Services.

2.5 DigiNotar B.V. (DigiNotar)

The private limited liability company within the DigiNotar partnership that is responsible, in a technical sense, for the DigiNotar Certificate Services offered through the DigiNotar partnership. DigiNotar B.V. is referred to in this CPS as: DigiNotar.

2.6 DigiNotar Certificate Services

The DigiNotar Services that relate to the issue and validation of DigiNotar Certificates or are directly associated with this.

2.7 DigiNotar Certificate Revocation List (DigiNotar CRL)

A file compiled and maintained by or on behalf of DigiNotar, which lists all the Certificates revoked by DigiNotar, insofar as they have not lost their validity due to expiration. The DigiNotar Certificate Revocation List is referred to in this CPS as: DigiNotar CRL.

2.8 DigiNotar Directory (LDAP Directory)

A file compiled and maintained by or on behalf of DigiNotar that includes the Certificates issued by DigiNotar. The DigiNotar Directory is referred to in this CPS as: LDAP Directory.

2.9 DigiNotar partnership

The partnership of the notarial profession to provide notarial TTP and associated services.

2.10 DigiNotar Services

The DigiNotar Certificate Services and DigiNotar Trust Services which are offered by the DigiNotar partnership.

2.11 DigiNotar Trust Services

The DigiNotar Services which are offered as TTP Services by DigiNotar in addition to the DigiNotar Certificate Services.

2.12 DigiNotar TTP civil-law notary

A civil-law notary who is a member of the DigiNotar partnership and who carries out TTP services such as verifying the data to be included in Certificates.

2.13 Electronic signature

A signature that consists of electronic data that is attached to or logically associated with other electronic data, and which is used as a means of authentication.

2.14 Encryption

A process in which data is encoded using a mathematical algorithm and a Key Pair, so that it cannot be read by unauthorised persons.

2.15 Public holiday(s)

Good Friday, Easter, Ascension Day, Whitsun Day, Queen's Day (30 April), Liberation Day (5 May), St. Nicholas Day (5 December), New Year's Day (1 January), Christmas and Boxing Day (25 and 26 December.)

2.16 User(s)

The natural person(s) for whom the authority is granted by or on behalf of the Client for the actual use of the DigiNotar Services provided. The User is not necessarily the Client.

2.17 Hash value

The unique control number that is a product of a calculation using a mathematical algorithm with the value of symbols and positions in an electronic data file.

2.18 Key archiving

The secure storage of the Private Encryption key by the Registration Authority or Certification Authority.

2.19 Online Certificate Status Protocol (OCSP)

The standard protocol that is used to Validate Certificates online. The Online Certificate Status Protocol is referred to in this CPS as: OCSP.

2.20 PIN code

A strictly personal code that allows the User to activate the Certificate provided and to use the Private Key associated with this Certificate. The PIN code is strictly personal and should be kept secret by the User, as long as the CPS does not state otherwise.

2.21 Private Key

A code generated using a mathematical program that must be kept strictly confidential by the rightful owner and which is uniquely linked with another generated code, the Public Key. The Private Key can be used to create an Electronic signature or to render encrypted electronic information readable.

2.22 Public Key

A code generated using a mathematical program that that is made public and which is used to verify an Electronic signature (which was made with the associated Private Key) or to encrypt electronic information (which can then only be rendered readable using the associated Private Key).

2.23 Registration Authority (RA)

A trusted authority that verifies the information needed for the application for the Certificate and, if approved, submits this information to the CA. In the DigiNotar partnership, the DigiNotar TTP civil-law notary is the Registration Authority. The Registration Authority is referred to in this CPS as: the RA.

2.24 Revocation Passphrase

A unique and strictly personal code (which is issued with the Certificate) that can be used to request the revocation of the Certificate.

2.25 Key Pair

A Public key and the associated Private Key, of which the functioning is inseparably linked.

2.26 Trusted Third Party (TTP)

A trusted, independent party, such as DigiNotar and the DigiNotar TTP civil-law notary in the DigiNotar partnership, that offers services to increase the reliability of the electronic data exchange. The Trusted Third Party is referred to in this CPS as: the TTP.

2.27 Validation

The checking of Certificates for:

- Whether the Certificate has been revoked; and/or

- The period of validity.

2.28 Verification and Identification System (VIS)

An inquiry system of stolen, missing or otherwise invalid unique identity documents and documents of value. The Verification and Identification System is referred to in this CPS as: the VIS.

2.29 Password

A combination of numbers, letters and/or symbols that the User, who generates the Key Pair, uses to secure the self-generated Private key.

2.30 Workday(s)

Calendar days, not including weekends and public holidays, on which the services described will be performed during 52 weeks a year.

3. Certificates

3.1 Organisation of the DigiNotar partnership

The DigiNotar Certificate Services are provided through the partnership between the DigiNotar and TTP civil-law notaries who are members of DigiNotar. DigiNotar and the DigiNotar TTP civil-law notary each have their own job in the provision of the DigiNotar Certificate Services. The DigiNotar TTP civil-law notary is responsible for the notarial part of the services provided and for his/her activities as RA. DigiNotar is responsible for the technical realisation of the services provided and for its activities as CA.

3.2 DigiNotar as the CA in the DigiNotar partnership

As part of the DigiNotar partnership, DigiNotar is a CA in electronic messaging. It is a Trusted Third Party who, in an environment in which the parties cannot see or hear one another, can offer certainty about the parties' identity and also their authority. DigiNotar provides such services as the issue, modification, renewal, and revocation of Certificates. Before it performs the services listed here, control measures (verifications) are performed by the DigiNotar TTP civil-law notary as the RA as described in this document.

3.3 Services provided by the DigiNotar TTP civil-law notary

As RA, the DigiNotar TTP civil-law notary can advise the Client, depending on the information provided by the Client, with regard to the Certificate types, in conjunction with:

a. The extent of confidentiality and/or security of the electronic messages to be sent;

b. The monetary value of the transactions to be performed with the electronic messages;

c. The evidence position (legal and otherwise) and the storage obligations with respect to the tax inspectorate, EDP auditors and other supervisory bodies;

d. The electronic messaging with foreign parties;

e. Key archiving.

The Client is responsible for the selection of the Certificate type, the use thereof and the results obtained, also in combination with other TTP services. The Client is free with respect to the choice of Certificate.

3.4 Certificate types

A distinction is made between the following types of Certificates:

a. Natural Person Certificate

b. Company Certificate

c. Person-specific Organisation Certificate/Person-specific Company Certificate

d. Professional Certificate (replaced by qualified Professional Certificate in 2005)

e. Professional Substitute Certificate (replaced by qualified Professional Certificate in 2005)

f. Envelope Certificate

g. Business Relation Certificate

h. SSL Server Certificate

i. Extended Validation SSL Certificate (new in 2006)

j. Signing Server Certificate

k. Software Signing Certificate

3.4.1 Functions and applications of Certificates

Unless indicated otherwise in this paragraph, the PIN code and Revocation Passphrase provided with the Certificate are strictly personal and made available in readable form only to the User stated in the Certificate.

The Natural Person Certificate is a Certificate that is used to identify a natural person and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User.

The Company Certificate is a Certificate that is used to immediately identify the natural person's authority to represent an organisation and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User.

The Person-specific Organisation Certificate, also called the Person-specific Company Certificate, is a Certificate used to identify a natural person as an employee of an organisation and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User. The Client and User are responsible for the actual existence of the employee relationship demonstrated by the Certificate.

The Professional Certificate is a Certificate that is used to identify a natural person as a practitioner of an independent profession and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User.

The Professional Substitute Certificate is a Certificate that is used to identify a natural person as a substitute of a professional active in the profession stated in the Certificate and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User.

The Envelope Certificate is a Certificate that is used to identify an organisation or a department in an organisation and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the Users. The PIN code and Revocation Passphrase provided with the Envelope Certificate are not personal and may be known by several Users.

The Business Relation Certificate is a Certificate intended to be used exclusively within a closed group defined by the Client, possibly in combination with a database kept by or on behalf of the Client, a business relation of the Client (such as a client or department thereof, a supplier, another company in the sector, a project participant, an employee), to identify this party within

the closed group and to guarantee the integrity and/or confidentiality of the electronic data exchanged by the User. The Client is responsible for the accuracy of the business relation's information included in the Certificate and/or the database and for this party's relationship with the User of the Certificate. The Client may choose whether the Certificate is based on the code or the name or the department of the organisation. The Client determines to whom the PIN code and the Revocation Passphrase are made available.

The SSL Server Certificate is a Certificate that is used to identify the domain name or the IP address of a Client server and also to create a secure connection with this server. The Revocation Passphrase delivered with the Certificate and the PIN code provided (upon generation of the Key Pair by DigiNotar) are made available exclusively to the Client.

The Extended Validation (EV) SSL Server Certificate is a Certificate that is used to identify the domain name or the IP address of a Client server and also to create a secure connection with this server. The Revocation Passphrase delivered with the Certificate and the PIN code provided (upon generation of the Key Pair by DigiNotar) are made available exclusively to the Client. A separate verification procedure applies for the EV SSL Server Certificate in accordance with the guidelines of the CA/Browser Forum as described below.

The Signing Server Certificate is a Certificate that is used, by running an application on a server of an organisation or a department thereof, to identify this department and/or organisation, as a user of the server. The Revocation Passphrase delivered with the Certificate and the PIN code provided (upon generation of the Key Pair by DigiNotar) are made available exclusively to the Client.

The Software Signing Certificate is a Certificate that is used to electronically sign software, in order to identify it as originating from the organisation or a department thereof that makes this software available. The PIN code and Revocation Passphrase provided with the Certificate are made known exclusively to the Client.

3.5 Custom Certificates

In consultation with DigiNotar, Certificates can also be created with different certificate specifications and/or a different distribution process than for the Certificate types as stated in section 3.4 of the CPS. These Certificates are specifically aligned with the individual needs of the Client and are called Custom Certificates. Custom Certificates have whatever legal consequences that the Client wishes to grant them.

3.6 Transfer of ownership of Certificate not permitted

The Client receives the right to use the Certificate and the Key in accordance with the provisions in this CPS. The Certificate remains the property of DigiNotar.

4. Applying for a Certificate

4.1 Application process

The application for the first Certificate must always take place in writing to ensure that the identity of the Client or the Client representative can be established personally. Any subsequent applications can be submitted either in writing or electronically, insofar as this is permitted by DigiNotar, taking account of the CPS and the policy regulations drawn up by DigiNotar.

4.2 The DigiNotar TTP civil-law notary as Registration Authority (RA)

The DigiNotar TTP civil-law notary is the RA in the DigiNotar partnership. The RA is responsible for the verification of the identity of the Client and/or the User and the other data to be included in the Certificate, to the extent that verification is required by the CPS. Applications for Certificates from a Client located in the Netherlands must also be submitted to an RA. If the application is made for a Client outside the Netherlands, this party's identity can be determined by a local civil-law notary or a comparable authority, this all being determined by the RA where the application is submitted.

The RA will only accept the application if the identity of the Client and/or the User stated in the Certificate – and this party's authority where necessary – has been sufficiently established. The RA is authorised to improve, upon performing the controls, any apparent writing errors, mistakes or omissions made when filling in the requested information, insofar as these improvements do not affect the content of the application.

The RA is authorised to refuse a request for the issue, change, renewal or revocation of a Certificate if the outcome of the verification and control procedure performed under the responsibility of the RA is inadequate. In that case, the Client will be contacted as quickly as possible.

The RA shall ensure that the Certificate is issued as quickly as possible and within the established term after the application for the Certificate has been submitted.

4.3 Verification

4.3.1 Generic verification

Before the issue of the first Certificate, the following control measures will be carried out (except for the stated exceptions, and independent of the type of Certificate):

1. The Client or the Client's representative will be identified under the responsibility of the RA.

2. The following information from the Client or the Client's representative will be checked:

a. Using a valid identification document:

- Surname and any prefixes;
- First name (in full);
- Middle name initials;
- Date of birth;
- Place of birth;
- Number of identity document;
- Validity of identity document.

b. If there is reason for the following, based on the VIS:

- Whether the identity document presented by the Client or the Client's representative has been reported as missing or stolen.

3. In addition to the above, the following information is checked for Clients that are organisations:

Using an excerpt from the register of the Chamber of Commerce where the Client is registered, or, in the case of organisations that do not register with the Chamber of Commerce, with the applicable registrations for this purpose, and/or based on relevant documents, or, in the case of public law organisations, using the applicable public law regulations, and/or on the basis of relevant documents:

- Authority to represent the Client;
- Business name;
- Name under the articles of association (only for organisations governed by articles of association);
- Address (business address and postal address);
- Registered office (only for organisations governed by articles of association);
- Registration number at the Chamber of Commerce (only for organisations registered with the Chamber of Commerce);

A copy of the identity document referred to in this document may be submitted. The other documents should be submitted as originals as far as possible.

4.3.2 Specific verification

In addition to or in deviation from the generic controls stated in section 4.3.1, there are still a number of certificate-specific control measures that are often performed, which are described in sections 4.3.2.1 to 4.3.2.6 of the CPS insofar as applicable.

4.3.2.1 Verification of Natural Person Certificate

For an application for a Natural Person Certificate, the RA may decide whether to check the following with regard to the Client, using the relevant documents:

- Street address;
- Postal code and city/town;
- Country of residence.

4.3.2.2 Verification of Person-specific Organisation Certificate/Person-specific Company Certificate

For an application for a Person-specific Organisation Certificate/Person-specific Company Certificate, the control measures described in section 4.3.1 sub 2 are performed for the intended User of the Certificate.

The application request may also be made electronically, provided an electronic means of identification is used, and which is based on an issuing procedure equivalent to the issuing procedure for Person-specific Organisation Certificates/Person-specific Company Certificates.

4.3.2.3 Verification of Professional Certificate, Professional Substitute Certificate

For an application for a Professional Certificate and Professional Substitute Certificate, the control measures described in section 4.3.1 sub 1 and 2 are performed for the intended User. For the application, the applicant should report in person to the RA and present an original identity document, or the applicant's identity should be determined on the basis of a legally accepted method, such as authentication of the signature by a civil-law notary.

In addition, when the Certificate is issued, it will be checked whether the intended User of the Professional Certificate actually practices the profession in question and/or if the intended User of the Professional Substitute Certificate is potentially authorised to temporarily or permanently act on behalf of the profession stated in the Certificate. These last checks will be performed by DigiNotar.

4.3.2.4 Verification of Envelope Certificate

For an application for an Envelope Certificate, the control measures described in section 4.3.1 sub 1 and 2 will be performed. For an application for an Envelope Certificate, each person registered with the Chamber of Commerce for the organisation in question, except for those persons not authorised to be representatives, is considered to be independently authorised in this regard.

4.3.2.5 Verification of Business Relation Certificate

For an application for a Business Relation Certificate, the DigiNotar TTP civil-law notary and/or DigiNotar do not perform any controls with regard to the intended Users (the business relations) of the Certificate. The Client is responsible for the accuracy of the information about the User which is included or not included in the Certificate.

4.3.2.6 Verification of SSL Server Certificate and Signing Server Certificate

4.3.2.6.1 General

For an application for a Server Certificate, the control measures stated in section 4.3.1 sub 1 and 2 are performed as far as applicable. If the Client and/or the User generates the Key Pair associated with the Certificate, then the RA verifies, using a unique identifying characteristic assigned to the electronic and written part of the application by the Client and/or the User, whether the written and electronic part of the application has originated from the same Client and/or User (see section 4.1 of the CPS.)

4.3.2.6.2 Verification of SSL Server Certificate PLUS

For an application for an SSL Server Certificate PLUS, the control measures stated in section 4.3.1 sub 1 are performed for the legal representative of the Client, and the control measures stated in section 4.3.1 sub 2 for the Client.

With regard to the Client's authorised representative who performs activities with respect to the Certificate on behalf of the Client, also known as the 'certificate administrator', the control measures stated in section 4.3.1 sub 1 are performed. For this purpose, for the application, the certificate administrator should report in person to the RA and present an original identity document, or the certificate administrator's identity should be determined on the basis of a legally accepted method, such as authentication of the signature by a civil-law notary.

For an application for an SSL Server Certificate PLUS, an independent registration service checks whether the Client is registered as the owner of the domain name or the IP address provided. If it emerges that the domain name or the IP address provided belongs to another organisation than the Client, then the Client must provide a statement that demonstrates that permission has been obtained from this organisation to use the domain name and/or the IP address.

4.3.2.6.3 Verification of SSL Server Certificate BASIS

For an application for an SSL Server Certificate BASIS, the control measures stated in section 4.3.1 sub 1 are performed for the Client's legal representative, and the control measures stated in section 4.3.1 sub 2 for the Client.

With regard to the Client's authorised representative who performs activities with respect to the Certificate on behalf of the Client, also known as the 'certificate administrator', the control measures stated in section 4.3.1 sub 1 are performed.

For an application for an SSL Server Certificate BASIS, an independent registration service checks whether the Client is registered as the owner of the domain name or the IP address provided. If it emerges that the domain name or the IP address provided belongs to another

organisation than the Client, then the Client must provide a statement that demonstrates that permission has been obtained from this organisation to use the domain name and/or the IP address.

4.3.2.6.4 Verification of EV SSL Server Certificate

For an application for an EV SSL Server Certificate, the control measures stated in section 4.3.1 sub 1 are performed for the Client's legal representative, and the control measures stated in section 4.3.1 sub 2 for the Client.

With regard to the Client's authorised representative who performs activities with respect to the Certificate on behalf of the Client, also known as the 'certificate administrator', the control measures stated in section 4.3.1 sub 1 are performed. For an application for an EV SSL Server Certificate, an independent registration service checks whether the Client is registered as the owner of the domain name of the IP address provided.

For an application for an EV SSL Server Certificate, an extra control measure will be performed by telephone to the number provided by the Client. One goal of this check is to ensure that the telephone number provided is the same as the telephone number of the location where the company is operated.

In any case, the above-mentioned controls and the other controls to be conducted are performed while talking into account the most recent guidelines in the 'Guidelines for Extended Validation Certificates' (drawn up by the CA/Browser Forum and published at: http://www.cabforum.org) which are set out as mandatory (and generally designated in the Guidelines by MUST) and taking into account the instructions in which certain issues are expressly forbidden (generally designated in the Guidelines by MUST NOT). To this extent, the Guidelines for Extended Validation Certificates apply directly to the issue of EV SSL Server Certificates.

The Guidelines for Extended Validation Certificates are published on the DigiNotar website. Insofar as a difference arises at any time between the applicable version published by the CA/Browser Forum and the version published on the DigiNotar website, the version published on the CA/Browser Forum shall prevail.

4.3.2.6.5 Verification of Signing Server Certificate PLUS (person-specific/not person-specific)

For an application for a Signing Server Certificate PLUS, the control measures stated in section 4.3.1 sub 1 are performed for the Client's legal representative, and the control measures stated in section 4.3.1 sub 2 for the Client.

With regard to the Client's authorised representative who performs activities with respect to the Certificate on behalf of the Client, also known as the 'certificate administrator', the control measures stated in section 4.3.1 sub 1 are performed. For this purpose, for the application, the certificate administrator should report in person to the RA and present an original identity document, or the certificate administrator's identity should be determined on the basis of a legally accepted method, such as authentication of the signature by a civil-law notary.

Insofar as the Signing Server Certificate is person-specific, it must be demonstrated that permission has been granted by the person stated in the Certificate.

4.3.2.6.6 Verification of Signing Server Certificate BASIS (person-specific/not person-specific)

For an application for a Signing Server Certificate BASIS, the control measures stated in section 4.3.1 sub 1 are performed for the Client's legal representative, and the control measures stated in section 4.3.1 sub 2 for the Client.

With regard to the Client's authorised representative who performs activities with respect to the Certificate on behalf of the Client, also known as the 'certificate administrator', the control measures stated in section 4.3.1 sub 1 are performed.

Insofar as the Signing Server Certificate is person-specific, it must be demonstrated that permission has been granted by the person stated in the Certificate.

5. Issue, acceptance, period of validity, change and renewal of Certificates

5.1 Issue

After verification and approval of the information as provided by the Client and/or User, the RA is responsible for preparing the Certificate. The Certificate can be provided in the following ways.

If the CA generates the Key Pair associated with the Certificate, the Certificate is activated using a PIN code to be given to the Client or the User, possibly with one or more security methods such as biometrics. This PIN code is sent to the Client or the User(s) designated by the Client in encrypted form, which is only readable to the User.

If the Client or the User generates the Key Pair associated with the Certificate, the Certificate is activated using a PIN code or Password that the Client or the User him/herself has given to the Key Pair in question, possibly with one or additional security methods such as biometrics. The Client or the User must treat this PIN code/Password in the same way as a PIN code provided by the CA. The Certificate is made available in writing in a sealed envelope directly to the Client or the Client's representative or in the form of a signed e-mail directed to the Client or the Client's representative.

The moment that the CA creates a Certificate applies as the date and time of issue of the Certificate. This date and time of issue of the Certificate are shown in the log files in the issue process recorded by the CA. These log files serve as evidence between the CA and/or the RA and/or the Client and/or vis-à-vis third parties. The date and the time that the Certificate is activated are not relevant for determining the date/time of issue.

The CA shall publish the Certificate in the DigiNotar certificate database (LDAP Directory).

5.2 Acceptance

The Certificate is considered to be accepted by the Client at the time of issue. The Client and User are obliged to check the information in the Certificate for accuracy before using the Certificate.

If an error is observed in the Certificate issued or the issue procedure, the Client or the User is obliged to submit a request for change by return mail, in accordance with the provisions of section 5.4 of the CPS.

Errors in a Certificate that has not been revoked are for the account and risk of the Client, which does not prejudice the liability of the CA and the RA with regard to shortcomings attributed to them.

The Client shall ensure that the Users, who are going to use the Certificate requested for them by the Client, are familiar with and in agreement with the CPS. Both the Client and the User are responsible for proper compliance with the CPS.

5.3 Period of validity

The Certificate is issued for a maximum period of validity of four years, commencing at the time of issue. The period of validity for the Certificate is stated in the Certificate.

Without prejudice to the Client's own responsibility to request a new Certificate in a timely manner, the User will receive, as a service, a standard e-mail no later then six (6) weeks in advance concerning the expiry of the period of validity of the Certificate.

For the obligations and legal and other consequences associated with the expiry of the maximum or other period of validity, please refer to sections 6.5 and 7.2.1 sub b of the CPS.

5.4 Change and renewal

A request for change or renewal of a Certificate must be made by the Client. The request may be made in the form of an electronically signed message (using a Certificate recognised by DigiNotar) or in writing, and directed to the RA or the CA.

The RA and/or the CA will not honour the request for change if, in his/her exclusive opinion, the controls performed have not produced the desired result. In this case, the Client will be informed of this as soon as possible.

If the Certificate is changed or renewed, a new Key Pair and Certificate will be generated and provided to the Client.

6. Revocation and validation of revoked Certificates

6.1 Revocation: general

The revocation of a Certificate involves the Certificate being rendered permanently inoperative. As such, it can no longer be considered reliable.

6.2 Request for revocation: general

A request must be submitted in writing or on the basis of a valid DigiNotar Certificate from the person authorised for revocation (see section 6.3 of the CPS), and may be directed to DigiNotar or the DigiNotar TTP civil-law notary.

The Client or the User may independently submit a request for revocation for the Certificate provided to him/her, using the Revocation Passphrase associated with the Certificate. The Client must fill in the relevant form on the DigiNotar website for this purpose. No controls will be performed on this request by the DigiNotar TTP civil-law notary. The Client and/or the User are required to keep the Revocation Passphrase strictly confidential.

The RA and/or the CA will not honour the request for revocation if, in his/her exclusive opinion, the controls performed have not produced the desired result. In this case, the Client will be informed of this as soon as possible.

The RA will immediately inform the CA of a request for revocation of the Certificate and shall request that a report of the revocation be made in the DigiNotar CRL as soon as possible.

The acknowledgement of receipt that the CA creates based on a request for revocation of the Certificate shall serve as evidence between the parties of the date and time of the request for revocation of the Certificate.

The CA will process a request for revocation exclusively during office hours on Workdays (see section 10.1 of the CPS), within three hours after receipt, and subsequently publish this on the DigiNotar website. Outside of office hours or Workdays, requests for revocation of a Certificate are considered to be received at the start of the subsequent Workday.

A request for revocation not made with the Revocation Passphrase provided must be made by a person who has been demonstrated to be authorised for this purpose. The request must be complete before the handling term commences.

6.3 Persons authorised for revocation

The Client and the User referred to in the Certificate may at all times submit a request for revocation concerning a Certificate issued at his/her request and/or on his/her behalf. A request for revocation by the Client or User is deemed equivalent to a request by the Client or User's representative or an heir of the person concerned.

The RA can revoke a Certificate based on the grounds referred to in section 6.5 of the CPS. A Certificate can be revoked by the CA based on the reason referred to in section 6.5 sub i of the CPS.

A Professional Certificate may also be revoked at the request of the relevant professional organisation (see section 6.5 sub d of the CPS.)

6.4 Obligation for revocation: Client, User

In any case, the Client or the User is required to submit a request for revocation in accordance with this CPS, if:

a. The data in the Certificate must be changed on the basis of incompleteness, inaccuracy or change of conditions, such as with respect to the User's authorities, and if the Client does not want to change the Certificate;

b. A Private key and/or the required access code for the Private key have/has been lost or have/has become known to an unauthorised person, or the Electronic signature otherwise no longer offers sufficient guarantees for the security of the electronic messaging sent on this basis;

c. Other urgent conditions to be reported to the RA.

It is the Client's responsibility to require his/her designated Users to immediately report a condition as stated above to the Client.

6.5 Grounds for revocation or request for revocation: RA, CA and Professional organisation

At the Client's first request, the RA is to revoke a Certificate that he/she has issued if the agreement concluded with the Client ends before the expiry of the period of validity stated in the Certificate.

In the following cases, the RA has the right to make a request for revocation and/or to dissolve all or part of the agreement with the Client by means of registered post sent to the Client without the need for legal intervention:

a. If the Client or the User has provided inaccurate or incomplete information about his/her identity or authorities;

b. In the case of a Professional Certificate, if the Client or the User no longer belongs to the professional group indicated, or the relevant professional organisation has suspended him/her from practicing the profession;

c. In the case of a Professional Substitute Certificate, if the User referred to in the Professional Certificate is no longer authorised to act as a substitute of the party practicing the profession stated in the Certificate;

d. If the request is made by the professional organisation of the Client or the User for whom a Professional Certificate of Professional Substitute Certificate has been issued. This request must be issued according to the procedure described in section 6.2 of the CPS;

e. If the competent authorities, on the basis of statutory provisions or a court decision, request inspection of the data as stated in section 9.2 of the CPS;

f. If the Client, without the permission of the RA, transfers his/her rights and obligations from the agreement concluded with the RA to a third party;

g. If the Client or User fails to comply with any of his/her obligations arising from this document or from the contractual agreements of which this document may form a part;

h. If the Client or User otherwise acts in such a way that the careful use of the Certificate is no longer guaranteed in the opinion of the RA;

i. If the DigiNotar partnership ends, or is changed in such a way that the RA can no longer be required to continue his/her services as set out in this document and the associated contractual agreements;

j. If, based on technical considerations, adequate security is no longer present;

k. If the agreement with the Client ends before the expiry of the period of validity stated in the Certificate.

In addition to the RA who issued the Certificate in question, in the cases referred to in section 6.5 sub b and c, the person charged with checking the professional register also has authority in this capacity, and in the case described in section 6.5 sub i and k, the CA also has this authority.

6.6 Grounds for revocation or request for revocation: RA, CA and Extended Validation Certificates

Reasons for revocation are defined in section 27 of the Guidelines for Extended Validation Certificates.

In addition to the general reasons for revocation stated in this CPS, the reasons for revocation below have been set out explicitly in connection with the regulations for Extended Validation (EV) Certificates.

The CA shall revoke the Certificate if:

- The CA suspects that the Private key has been compromised;
- The CA is informed that the certificate holder (subscriber) is no longer the owner of the domain for which the EV Certificate was issued;
- The Certificate was not issued in accordance with EV guidelines;
- The CA no longer has the right to issue EV Certificates, unless agreements have been made to continue the revocation status service;
- The private key of the EV CA has been compromised;
- The certificate holder (subscriber) has been added to a valid ‘black list’ for the issue of EV Certificates or operates from a country that is not approved for EV Certificates according to the CA.

6.7 Verification of request for revocation

With regard to a request for revocation, the person submitting the request will have his/her information as stated in section 4.3.1 sub 2.a. of the CPS verified, along with the basis for his/her authority. Copies of any and all relevant documents may be requested for this purpose.

6.8 Revocation of Certificates

DigiNotar assesses whether a certain Certificate can be revoked. A Certificate is considered to be revoked once the revocation has been published on the DigiNotar website.

6.9 Consequences of the revocation

6.9.1 Client and User

After the revocation of a Certificate, the User is obliged to cease using the Certificate and the associated Key Pair. If the User violates this ban, then the DigiNotar TTP civil-law notary may confirm to the Client and/or the User that this person is in default, and demand that he/she refrain from further violation of the ban. If the Client and/or the User does not comply with this demand, then he/she is liable to pay a fine payable on demand for each violation, amounting to ten times the DigiNotar recommended price of the issue of the type of Certificate that has been revoked, without prejudice to DigiNotar TTP civil-law notary's right to collect complete reimbursement of the damages resulting from the violation.

6.9.2 The party relying on the Certificate

The result of the revocation of the Certificate is that a third party relying on the Certificate, as in cases described in section 7.2.1 sub a of the CPS DigiNotar, is *not* entitled vis-à-vis the Client and/or the User to rely on the legitimate confidence in the Certificate.

6.10 Validation of revoked Certificates

DigiNotar publishes a list of revoked Certificates. The information published in the DigiNotar CRL about revoked Certificates can be consulted in a variety of ways. The Client is responsible for the way in which he/she decides to Validate Certificates.

The following validation methods are offered:

1) Website validation

2) OCSP validation

3) CRL validation

6.10.1 Website validation

Website validation is the method that makes information on revoked Certificates available to *everyone* on the DigiNotar website. Interested parties can validate the Certificate by retrieving the data for the Certificate in question, by means of a search method offered on the DigiNotar website. The website publication is always up to date and is indicative of the time of revocation.

6.10.2 OCSP validation

OCSP validation is an online validation method in which DigiNotar sends the Client an electronically signed electronic message (OCSP response) which states the status of the Certificate requested by the Client and/or User. The information provided in the OCSP validation is equivalent to and as up-to-date as the information published on the DigiNotar website. If an OCSP response is absent, no conclusions can be drawn from this situation.

6.10.3 CRL validation

CRL validation is a validation method in which DigiNotar can provide a copy or an excerpt from the published DigiNotar CRL that shows whether a Certificate has been revoked or has lost its validity. The copy or excerpt from the DigiNotar CRL does not necessarily contain the same information as the most up-to-date information published on the DigiNotar website.

The DigiNotar CRL used for the CRL validation is never more than 25 (twenty-five) hours older than the current CRL. The risk as to whether the information is up to date is borne by the person using the CRL validation.

7. The use of the Certificate and third parties relying on the Certificate

7.1 The use of the Certificate

7.1.1 Obligations of the Client/User

From the moment that the Certificate is used, the Client and the User are responsible for the management of the Private key, the information recorded in the Certificate, the personal PIN code provided to him/her, and the self-generated Password or PIN code associated with the Key Pair, in accordance with the CPS and the contractual agreements of which the CPS can form a part.

From the moment that the Certificate is used, the Client and, as far as possible, the User, will carefully manage the Private key and take technical, HR and organisational measures to secure the Private Key and the Client's system against loss or theft and unauthorised use, in any way whatsoever.

The Client and the User must inform the RA in a timely manner in writing (post, fax, signed e-mail) about every change important for the Certificate issued, such as changes in the name, domain name, address, e-mail address, residence (name/address/residence information), and authorities and any changes to the legal form of the company, all of this insofar as this information is known by the Client and/or the User.

In all cases, the Client is liable for damages arising from the late revocation or change of the Certificate, after the issue of the Certificate, regardless of whether the need to revoke or Change the Certificate can be attributed to the Client.

The Client and the User must report the loss, theft or unauthorised use of the Private Key, personal PIN code, and Password provided to him/her as well as irregularities in the Client's system or other relevant conditions to the RA immediately upon discovery of the situation.

7.1.2 Client obligations to the Users for whom the Certificates have been requested

The Client is responsible for ensuring that the Certificate(s) and PIN mailer(s) provided to him/her are given to the User(s) indicated on the token(s)/PIN mailer(s). To this end, the Client shall, before the issue of the Certificate(s) and PIN mailer(s), be certain of the identity of the User(s). The Client shall ensure that the User(s) of a Certificate issued to the Client are familiar with and in agreement with the CPS. Both the Client and the User are responsible for proper compliance with the CPS with respect to the Users(s) for whom he/she requested the Certificates.

The Client must ensure that:

a. A User shall always carefully use the Private key and the access thereto, keep these strictly confidential, and save them with Encryption, which is secured with a PIN code to be kept secret by the User;

b. A User only uses the Certificate for the purpose for which the Client is authorised and duly takes the associated limitations into account;

c. A User does not use the Certificate in a way that is in conflict with the provisions in this document or the associated contractual regulations;

d. A User has the right to use the business name, brand name and logos referred to in the Certificate.

7.1.3 Limitations in use

The Client shall abide by the applicable Dutch, European and other national and international legislation and regulations and the provisions of the CPS with regard to the purpose for which he/she wishes to use the Certificate, the choice of the other party with whom he/she exchanges electronic messages and, more specifically, the content of the messaging that he/she wishes to carry out using the Certificate. This also includes agreements concluded by him/her with consumers and the Encryption he/she has used. The Client and the User(s) are forbidden to use the Certificate for purposes other than stated in the CPS.

The Client shall indemnify the DigiNotar partnership, DigiNotar, the DigiNotar TTP civil-law notary and the civil-law notary office of which the DigiNotar TTP civil-law notary is a part from any and all legal action from a third party based on the assertion that the content of the electronic messaging does not comply with applicable Dutch, European and other national and international legislation and regulations, especially with regard to the agreements he/she has concluded with consumers, the Encryption he/she has used and, furthermore, everything else that relates to the content of the electronic messaging.

7.2 The third party relying on the Certificate

7.2.1 General

The third party with whom the Client and/or the User exchanges electronic messages is not entitled vis-à-vis the Client to rely on the legitimate confidence in the Certificates if, immediately prior to the reliance on the Certificate:

a. The Certificate has been revoked, according to the information published on the DigiNotar website (see section 6.7 of the CPS); or

b. The validity of the Certificate has expired, according to the period of validity stated in the Certificate; or

c. The third party has not taken any account of the limitations in the use of the Certificate as referred to in the CPS and/or the Certificate and/or the consequences associated with the use of the Certificate; or

d. The third party does not take into account the measures required in the CPS or other agreements.

7.2.2 Limitation of liability of the RA and CA

Without prejudice to the Client's responsibility, the RA and/or CA, insofar as it relates to him/her, only guarantees the content of the Certificate vis-à-vis third parties at the time of issue, as referred to in this CPS and exclusively for the information that must be verified in accordance with this CPS.

7.2.3 Limitation of legal and other consequences for Business Relation Certificate, Envelope Certificate and Custom Certificate

There are no other legal consequences associated with the use of the Envelope Certificate, Business Relation Certificate and the Custom Certificate other than identification of the Client and/or User stated in the Certificate.

As a result of this use, third parties are also not entitled to rely on the creation of obligation and/or the ability to attribute obligations to the Client, unless these third parties form a closed group with the Client, in which case the legal consequences of the closed use will be determined on the basis of explicit agreements between the Client and the group members.

8. Intellectual and industrial property rights

The intellectual and industrial property rights, which include copyrights and trademark rights, that are used in relation to the DigiNotar Certificate Services or form part of the DigiNotar Certificate Services, which expressly includes the software used for creating and activating Certificates with Key Pairs, as well as documentation, manuals and their translations, are vested in DigiNotar or its suppliers. If the intellectual property rights are vested in a supplier of the CA or of the RA, the CA or RA respectively guarantees, to the extent relevant to each of them, that it is authorised to grant the licence for the use of the software subject to the relevant licence terms.

The Client or the User only acquires the rights of use and authorities granted to it under the present terms or otherwise expressly granted during the term of this agreement. It will otherwise not reproduce or produce copies of the software or other materials. Upon termination or dissolution of the agreement, the Client or the User must return the software (including its carriers), as well as any documentation, manuals and translations thereof.

The Client may not remove any mention of copyrights, trademarks, trade names or other intellectual or industrial property rights from the software, the equipment or the materials or change these, including mention of the confidential nature and secrecy of the software.

The RA or the CA indemnifies the Client or the User against any claim from third parties based on the assertion that the RA or the CA is not authorised to grant licences for the software used in conjunction with the TTP services or that the software infringes the rights of third parties.

The RA uses the TTP products the CA has developed using the suppliers' software. These suppliers' licence terms can be obtained from the CA. The provisions of these licence terms are hereby declared applicable in full to the agreement concluded with the Client. In the event of conflict between these licence terms and another document, including the CPS, the licence terms will prevail.

9. Key archiving

9.1 General

In the event of Key Archiving, DigiNotar generates two Key Pairs for the Client. The Key Pair for the Electronic Signature is immediately sent to the Client. Upon the Client's request, the DigiNotar TTP civil-law notary at DigiNotar may take custody of the Private Key of the Key Pair for Encryption or confidentiality. The Key Pair for Encryption can only be used to make a message readable or unreadable.

The custody may be terminated at all times upon the Client's request, made in writing or by electronically signed e-mail.

9.2 Making available of the Private Key for Encryption

If the DigiNotar TTP civil-notary is required to make the Private Key for Encryption taken into custody by DigiNotar available to the competent authorities on the grounds of any statutory provision or decision of a court of law, or he/she will immediately inform the Client thereof, unless he/she is prohibited from doing so under the relevant provision or decision of the court of law.

9.3 Term of the custody

Unless otherwise agreed upon with the Client, the Private Key for Encryption will be taken into custody for a term of two years. Upon expiry of this term, it may be renewed in mutual consultation for a term to be agreed upon at that time. DigiNotar will have the right to refrain from renewing the term of the custody for notarial or technical reasons.

9.4 Copy of the Private Key for Encryption

If it should become impossible for the Client to use the Private Key for Encryption, a copy of which has been taken into custody, the Client may request a copy of the relevant key. The DigiNotar TTP civil-law notary will only provide this copy to the Client, the User or an authorised proxy in person.

10. Other obligations, liability and indemnification

10.1 Obligations: DigiNotar and DigiNotar TTP civil-law notary

DigiNotar and the DigiNotar TTP civil-law notary will perform all their work as part of the CPS and the agreements of which the CPS may form part with due dispatch. Unless expressly agreed otherwise, DigiNotar and the DigiNotar TTP civil-law notary will perform their work on business days from 9 a.m. until 5 p.m.

The DigiNotar TTP civil-law notary will carry on his/her professional practice with due observance of DigiNotar's guidelines. As part of his/her TTP services, the DigiNotar TTP civil-law notary will organise his/her equipment, software, telecommunications facilities, systems administration and procedures in accordance with DigiNotar's guidelines. The DigiNotar TTP civil-law notary will exercise the greatest possible care in performing the verification and checking procedures on the basis of the information provided by the Client and/or the User, in conformity with the CPS.

10.2 Limitation and exclusion of liability: DigiNotar, the DigiNotar TTP civil-law notary and the DigiNotar partnership

10.2.1 Limitation and exclusion of liability: general

Any right to damages is always conditional upon the Client informing DigiNotar or the DigiNotar TTP civil-law notary of the relevant loss or damage by registered letter as soon as reasonably possible after it has been sustained. Any arrangements the Client or the User makes with other Clients, Users or third parties resulting in responsibilities that deviate from those customarily arising from the use of the Certificates will not result in more extensive responsibilities and/or liabilities on the part of the DigiNotar TTP civil-law notary and DigiNotar than would have been the case had such arrangements not been made.

The DigiNotar TTP civil-law notary and DigiNotar are only liable for the portion of the services of which it/he/she bears the cost, without prejudice to any limitations or exclusion of liability that might apply to them.

The DigiNotar TTP civil-law notary and DigiNotar do not guarantee the accuracy, authenticity, integrity and reliability of the information provided by the Client of the User that is not to be verified in conformity with this CPS, without prejudice to the fact that the relevant information may be attributed to the Client or the User.

10.2.2 Limitation of liability: DigiNotar and DigiNotar TTP civil-law notary

In the event of the issue, amendment, renewal or withdrawal of a Certificate, the DigiNotar TTP civil-law notary only warrants that:

a. The DigiNotar TTP civil-law notary performed the verification and checking procedure in accordance with the CPS;

b. The DigiNotar TTP civil-law notary did not make any mistakes in the issue, amendment, renewal or withdrawal of a Certificate that are due to his/her failure to exercise reasonable care in complying with the CPS;

c. A Certificate issued satisfies CPS requirements;

d. The information verified in accordance with this CPS as included in a Certificate, are accurate at the time of issue of a Certificate, but not necessarily thereafter.

The damages payable for the attributable failure to perform the agreement concluded with the Client will in no event exceed EUR 50,000 (in words: fifty thousand euros) for each event, subject to the maximum amount the relevant insurance company pays out in the event of a closely connected series of events, but never more than EUR 500,000 (in words: five hundred thousand euros).

In the event of a continuing performance agreement concluded with the Client, damages for such attributable failure will never exceed the price (excluding VAT) stipulated in that agreement for DigiNotar's and the DigiNotar TTP civil-law notary's services for the period covering 3 (three) months prior to the failure.

The total amount of DigiNotar's and the DigiNotar TTP civil-law notary's liability for loss or damage on account of death or bodily injury or for material damage to property will never exceed EUR 50,000 (in words: fifty thousand euros) for each event, with a closely connected series of events counting as a single event.

10.2.3 Exclusion of liability: DigiNotar, the DigiNotar TTP civil-law notary and the DigiNotar partnership

DigiNotar and the DigiNotar TTP civil-law notary cannot be held responsible for:

a. The accuracy and correctness of information not verified and/or checked that is not to be verified and/or checked in conformity with the CPS;

b. The issue of a Certificate based on incorrect information provided by the Client to the extent that the inferiority of such information could not reasonably have been discovered based on the checks required under this CPS;

c. Changes to the identity and/or authorisations of the Client and/or the User and their master data or other data following the issue of a Certificate;

d. The use of a Certificate after its issue. Liability is expressly excluded in the event that a fault in the message sent or an error in its dispatch or receipt causes serious loss or damage, such as bodily injury, death or environmental damage, including but not limited to the context of the use of nuclear systems, traffic and traffic control systems and medical applications;

e. The contents of the messages to be created in using the Certificate;

f. Loss or the theft or unauthorised use of the Client's or User's Private Key by third parties following the issue of a Certificate;

g. The use of a Certificate after its withdrawal;

h. Errors caused by the transmission of data by the Client and/or the User, the software, the equipment, or the telecommunications facilities used by the Client and/or the User.

DigiNotar and the DigiNotar TTP civil-law notary are not liable for delays and faults in the performance of work that are due to technical or other disruptions, such as transmission errors, disruptions in equipment and system software, faults in equipment and software, wilful misconduct such as fraud, the illegal use of software, sabotage and data theft, operating errors made by third parties, mistakes made by third parties resulting in network breakdown, power outages, fire, lightning strikes, significant water damage, a break in a telephone cable, acts of war, acts of God and, more generally, all causes unrelated to the reasonable care to be exercised by DigiNotar and/or the DigiNotar TTP civil-law notary.

Otherwise, DigiNotar and the DigiNotar TTP civil-law notary accept no other liability than that assumed under the CPS and their General Terms and Conditions of Delivery. Any and all liability of the DigiNotar partnership as such is hereby excluded in full.

10.3 Warranties and indemnification: the Client

10.3.1 Warranties provided by the Client

The Client hereby warrants that:

a. The information stated in the Certificate is correct and complete at all times;

b. The Certificate is used in compliance with the applicable statutory and other rules (e.g. data protection laws, the Dutch Civil Code, telecommunications laws);

c. The Certificate is used in accordance with the provisions of the CPS and the agreements of which the CPS may form part and that relate to the CPS;

d. The User(s) will duly comply with the provisions of the CPS and the contractual arrangements of which the CPS may form part.

The Client is responsible for its choice and (physical) security of its software, equipment and telecommunications facilities, as well as for the availability of its information and communications systems with which it realises electronic messaging. The Client will take appropriate action to safeguard its system against viruses and other elements alien to the software.

10.3.2 Indemnification by the Client

The Client indemnifies DigiNotar, the DigiNotar TTP civil-law notary and the DigiNotar partnership against all claims from third parties based on the assertion that the information stated in a Certificate issued by the DigiNotar TTP civil-law notary is no longer correct or complete.

The Client indemnifies DigiNotar, the DigiNotar TTP civil-law notary and the DigiNotar partnership with respect to all damage it might sustain as a result of claims from third parties relating to services provided or products supplied by DigiNotar and/or the DigiNotar TTP civil-law notary, unless they are attributable to wilful misconduct or gross negligence on the part of DigiNotar and or the DigiNotar TTP civil-law notary, except to the extent a specific party is liable under the CPS.

11. Miscellaneous

11.1 Applicable law and competent court

All agreements between the Client, the DigiNotar TTP civil-law notary and, to the extent applicable, DigiNotar will be governed by Dutch law. The Client hereby elects domicile at the offices of the DigiNotar TTP civil-law notary. All disputes arising from or relating to these agreements will be submitted for settlement to the court having jurisdiction in the place of establishment of the DigiNotar TTP civil-law notary or DigiNotar.

11.2 Invalidity

If any provision of any agreement between the Client and the DigiNotar TTP civil-law notary or DigiNotar is found invalid, this will not affect the validity and enforceability of the remaining provisions of that agreement. The parties will consult to agree as soon as practicable on a replacement provision that approximates the content and purpose of the invalid provision to the greatest extent possible.

11.3 Audit

A registered EDP auditor (RE) or an individual whose qualifications can be demonstrated to be equal, will each year verify compliance at DigiNotar and – on a sample basis – at the DigiNotar TTP civil-law notary with the requirements set out in the CPS, the legal provisions, the annexes to the CPS, the agreements of which the CPS may form part, as well as the security policy referred to in section 11.5 of the CPS. The audit referred to in this section will also be based on the relevant laws and regulations.

11.4 Privacy

The Client hereby grants the DigiNotar TTP civil-law notary and DigiNotar its permission to publish the Certificate's serial number, status information and information meant for publishing in DigiNotar's certificate databases, such as the LDAP Directory and the DigiNotar CRL.

The DigiNotar TTP civil-law notary or DigiNotar will ensure that the required technical and organisational arrangements are made to safeguard personal and other data against loss or infringement and against unauthorised access, amendment or provision of personal and other data.

In ensuring the security of the personal data, the DigiNotar TTP civil-law notary will comply strictly with the relevant laws and regulations.

11.5 Security policy

The DigiNotar partnership has laid down its security policy in action protocols and technical protocols. For safety reasons, these documents are not publicly available, which means that they are unavailable for inspection.

The audit referred to in section 11.3 of the CPS will also be based on these action and technical protocols.

11.6 Discontinuation of a DigiNotar TTP civil-law notary's services

If a DigiNotar TTP civil-law notary discontinues his/her services, the DigiNotar partnership will at all times ensure the continuation of the agreements then in force.

11.7 Changes to the CPS DigiNotar

The Client hereby acknowledges the CA's authority to make changes to the CPS. The changes will take effect after a term to be specified by the CA, which may not be less than four weeks, save in exceptional circumstances, following written notification or an electronically signed e-mail sent to the Client or publication on the DigiNotar website (www.DigiNotar.nl).

Changes of minor importance may be made without a specific term applying.

If the Client indicates in writing or by means of an electronically signed e-mail, within four weeks from the notification, that it does not agree to the change, this will be considered a request that the relationship be ended with immediate effect and the Certificates issued upon its request be withdrawn. The foregoing is without prejudice to contractual obligations still in force, unless the CA has made manifestly unreasonable changes.

11.8 Notifications and reports

All notifications and reports referred to in the CPS and in the agreements of which the CPS may form part may be made by electronic messaging (e-mail or website), unless expressly provided otherwise or requested otherwise by the DigiNotar TTP civil-law notary.

If a user or holder of an Extended Validation certificate, a trusting party or a party otherwise involved in the Extended Verification Certificates issued by DigiNotar wishes to file a complaint or report his/her suspicions of abuse, fraud, incrimination or other inappropriate conduct relating to such a Certificate, he or she may do so through the online help desk system. The foregoing does not relieve the party entitled to such an Extended Validation Certificate from the obligation to withdraw the Certificate where necessary. A report as referred to above will, as such, never be considered a withdrawal.