

P.O. Box 90420
2509 LK Den Haag
Phone + 31 70 3159232
Fax + 31 70 3159201

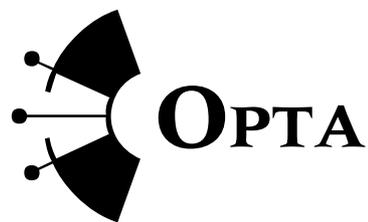
Before you start!

*This form **may only** be used to apply for registration of **the provision or issue of qualified certificates to the public** as referred to in Section 2.1 of the Telecommunications Act as amended in the Electronic Signatures Act (Staatsblad 199, 2003). Completion of this form facilitates quick processing of the registration and also serves as a guide in compiling the information file. The information file is a collection of information regarding the setup of the services provided to the public by a provider of qualified certificates. The information in this file forms the basis of the registration as well as future regulation of compliance with the legal obligations. The contents of the file consists of the answers to the questions and the relevant appendixes. A separate general explanation of this form is available¹. No detailed explanation per question is available for completion of the form, but the enclosed reference table and knowledge of the documentation referred to will help in answering the questions. This pertains to the following documents: General Ordinance 'Decision requirements electronic signatures' (Staatsblad 200, 2003), Ministry regulations 'Regulations electronic signatures' (Staatscourant 88, 8 May 2003), ETSI TS 101 456 'Policy requirements for certification authorities issuing qualified certificates'². With multiple choice questions, mark the correct response. If a response is explicitly requested in the form of an appendix, enter a reference to the relevant appendix(es) and page(s) on the form. In compiling the information file, OPTA strives to ensure that the applicant must compile as few specific documents as possible, but rather uses documents already available from the applicant in so far as possible. For proper accessibility of the requested/desired documents, the appendixes must be properly numbered and the references must be clear.*

¹ This explanation can be downloaded from the OPTA website: www.opta.nl.

² These documents can be downloaded from the OPTA website: www.opta.nl.

Certification service provider offering qualified certificates



A Applicant information

A1 Enter **all** data regarding your company, yourself, and address:

Name applicant _____
Company name

Department _____

Postal address _____

Postal code / city _____ Country _____

Visiting address
(if different) _____

Postal code / city _____ Country _____
(if different)

Chamber of Commerce registration number _____

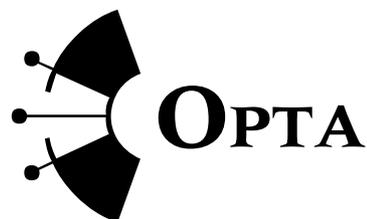
Contact person name, first initial(s) _____ m f

Position _____

Phone number _____ Fax number _____

E-mail address _____

Certification service provider offering qualified certificates



A2 A fee is due for registration and for being registered. The tariffs are determined by the Minister of Economic Affairs and change each year. They can be found on the OPTA website³. An invoice will be sent to you for this fee. If your organisation wishes to receive this invoice at a different location or department than that stated under A1, please indicate the invoice address below. If your organisation wants a payment reference code included on the invoice, please indicate this below.

Name
Company name _____

Department _____

Postal address _____

Postal code / city _____ Country _____

Contact person name, first initial(s) _____ m f

Phone number _____ Fax number _____

Your payment reference code _____

A3 Identification document

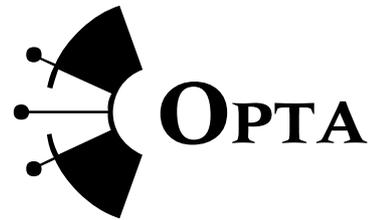
If your company is registered in the trade register, or in the register of associations or of foundations, you must enclose a copy of the registration for the information file. This excerpt may **not be more than six months old**. The excerpt must contain all information regarding the applicant and must **indicate the representation authority of the person signing this form**.

If the representation authority of the person signing this form is not evident from the excerpt, you must enclose

authorisation signed by a person whose representation authority is evident from the excerpt. If the party is not a company registered in the trade register (or the register of associations or foundations) but a 'private person', a copy of a valid passport must be enclosed together with an excerpt of the register of residency. Please indicate the location of the applicable documents in the information file.

³ These tariff regulations can be downloaded from the OPTA website: www.opta.nl.

Certification service provider offering qualified certificates



B Provider of qualified certificates

A general explanation of this application form can be separately downloaded from the OPTA website: www.opta.nl. This explanation also includes a list of terminology as used in this form. An explanation per question of how to complete this form is not available, but the enclosed reference table at the end of this form and knowledge of the documents referred to will be of assistance in answering the questions.

B.1 *In what way does your organisation make the provision of qualified certificates public or will it make this public?*

Provide in an appendix a brief summary of the manner in which, the media by means of which and the target groups to which (brochures, door-to-door periodicals, newspapers, magazines, radio, television, internet, etc.) your offer is made known, has been made known or will be made known. Enclose this appendix in the information file. Indicate below the name of the appendix and where it can be found in the information file (page numbers and paragraphs).

B.2 *Is it your intention to participate in PKI Government and do you satisfy or do you intend to satisfy the requirements of PKI Government?*

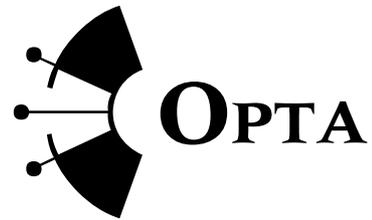
- Yes; does your organisation object to OPTA informing PKI Government of this intention?
 No
 Your organisation does not want to answer this question.

- No
 Yes

B.3 *The Commission for the protection of personal data (CBP) or a representative for data protection (FG) registered with the CBP must be informed that you process personal data. Has your organisation submitted such notification?*

- Yes, to the CPB; notification number: _____
 Yes, to an FG; name of the FG: _____
 No; OPTA will inform the CBP accordingly.

Certification service provider offering qualified certificates

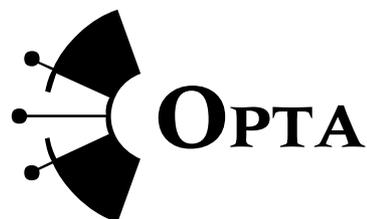


B.4 Supply a list with the addresses of all registration authorities (RAs) that your organisation uses. If your organisation has valid proof of evaluation for the provision of qualified certificates by an organisation appointed in accordance with Section 18.16 sub-section 1 of the Telecommunications Act as amended in the Electronic signatures Act (hereinafter: Tw) by the Minister of Economic Affairs, we request that you indicate per RA whether or not it was assessed in the evaluation. If such proof for the assessed RAs was issued, we request that you include copies in the information file. Include the requested list and proof in the information file and indicate below where these can be found in the information file (page numbers and paragraphs).

B.5 Does your organisation have valid proof of determination as referred to in Section 2.1 sub-section four of the Tw for the provision of qualified certificates issued by an organisation appointed in accordance with Section 18.16 sub-section 1 of the Tw by the Minister of Economic Affairs? If applicable, include a certified copy of a valid certificate issued by a certification institution as appendix (page numbers and paragraph(s)):

- Yes, go to part K and complete the form from there. Sign the application and include a certified copy of the proof in the information file. Also include with this form all communication made publicly available by your organisation to certificate holders and trusting parties, in any event including a model certificate, the general terms, PKI disclosure statement (PDS) and the Certification Practice Statement (CPS). If available, also include brochures and tariff lists.
- No; answer all questions in the following sections on this form for compilation of the information file. The intention of these questions is to compile the information file.

Certification service provider offering qualified certificates



C Liability and conditions

C.1 Based on which Qualified Certificate Policy (QCP), as identified in the standard ETSI TS 101 456 'Policy requirements for certification authorities issuing qualified certificates'⁴, does your organisation operate?

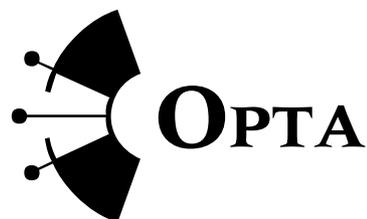
- QCP public + SSCD; Qualified Certificate Policy (QCP) for qualified certificates in which a secure device (SSCD) is required for the creation of electronic signatures.
- QCP public; Qualified Certificate Policy (QCP) for qualified certificates.
- other; indicate the rules you apply and include the standards you apply in the information file (page numbers and paragraph(s)): _____

C.2 How does your organisation indicate in its qualified certificates that it complies with the Qualified Certificate Policy (QCP) it applies?

Include the relevant procedure in which this is described in the information file and indicate below where this can be found in the information file (page numbers and paragraph(s)).

⁴ For additional information see ETSI TS 101 456 § 5.2.

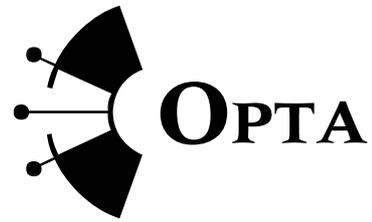
Certification service provider offering qualified certificates



C.3 *How does your organisation ensure that the general conditions for the use of qualified certificates are available to the certificate holders and the trusting parties? Complete the following table.*
 Include the general conditions and if applicable 'PKI disclosure statement' (PDS) for certificate holders and those for trusting parties in the information file. Location of general conditions and PDS in the information file:

<i>Which of the following items are covered by your general conditions or other documents?</i>	<i>Document name</i>	<i>Page</i>	<i>Paragraph</i>
1. <i>The Qualified Certificate Policy applied, including a clear statement whether the certificates are intended for the public and whether these rules require use of a secure device to generate electronic signatures.</i>			
2. <i>Any restriction on the use.</i>			
3. <i>Restrictions and financial limits on liability.</i>			
4. <i>The period of time that the certificate holder's registration data is stored.</i>			
5. <i>The period of time that the certificate provider stores his event logs (hereinafter: event logs).</i>			
6. <i>Procedures for dealing with complaints and conflicts.</i>			
7. <i>The applicable legal system.</i>			
8. <i>The existence of an optional accreditation system and whether your organisation is certified on the basis of this for working in accordance with the applicable Qualified Certificate Policy, and which certifying institution (organisation) awarded this certification.</i>			
9. <i>The information regarding how trusting parties can verify the validity of a qualified certificate, including the manner in which the list of suspended and revoked certificates (CRL) is to be used.</i>			
10. <i>Procedure for revocation of qualified certificates.</i>			

Certification service provider offering qualified certificates

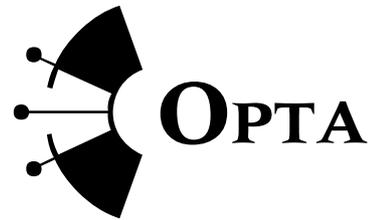


C.4 In what way does your organisation ensure that the contract parties and the certificate holders comply with the obligations listed below? Complete the following table.

Include the agreement, general conditions, if applicable the 'PKI disclosure statement' (PDS), and any other additional conditions in the file. Location of agreement(s), general conditions, PDS if applicable and any other additional conditions in the information file:

Which of the following items are covered by the agreement, the general conditions or any other additional conditions?	Document name	Page	Paragraph
1. The certificate holder supplies correct and complete information, especially with reference to the registration, that is in keeping with the rules applied.			
2. The certificate holder only uses his/her key pair for placing electronic signatures and acts in accordance with the restrictions that the certificate issuer has imposed upon the certificate holder.			
3. The certificate holder applies due caution in dealing with the private key in order to prevent abuse.			
4. If the contract party or certificate holder generates the certificate holder's key pair, this is done as follows: <ul style="list-style-type: none"> • with an algorithm that is considered suitable for qualified electronic signatures • with a key length and an algorithm that are considered suitable for qualified electronic signatures • only the certificate holder has access to the private key once it has been issued to the certificate holder. 			
5. If the Qualified Certificate Policy (QCP) requires use of a secure device (SSCD) (QCP public + SSCD), the qualified certificate may only be used in combination with advanced signatures that were generated with a secure device (called qualified electronic signatures).			
6. If the key pair is generated under the responsibility of the contract party and the Qualified Certificate Policy (QCP) requires using a secure device to generate electronic signatures (QCP public + SSCD), the key pair is also created within a secure device.			
7. The certificate holder immediately informs the certificate issuer of the following events that occur prior to the end of the validity of the qualified certificate: <ul style="list-style-type: none"> • the private key is or could be compromised or has been lost or stolen, or • the certificate holder has lost control of use of the private key because the activation data (e.g. PIN code) has been compromised or due to other reasons or causes, and/or • the qualified certificate contains incorrect data or the data content has changed from the content explained to the certificate holder. 			
8. Once the private key is compromised, the certificate holder immediately blocks the relevant certificate.			

Certification service provider offering qualified certificates



C.5 *How are trusting parties informed of the general conditions that apply and warned that the qualified certificate can be trusted providing the applicable minimal obligations are satisfied? Complete the following table.*

Include a copy of the content of a qualified certificate and the general conditions for the trusting party in the information file. Location copy of content of qualified certificate:

Which of the following items are covered by the certificate and/or in the general conditions?	Document name	Page	Paragraph
1. <i>The trusting party verifies the validity, suspension or revocation by using the revocation status list in the manner explained to the trusting party.</i>			
2. <i>The trusting party complies with every restriction in using the qualified certificate as explained as such in this certificate or in the general conditions.</i>			
3. <i>The trusting party takes all other precautions as explained in the agreements, the general conditions or elsewhere.</i>			

C.6 *How and when does your organisation communicate the general conditions to the contract parties and/or certificate holders and trusting parties, irrespective of use of the relevant qualified certificates, and in what way do you make these known in such a way that they can be read and understood and are available by means of sustainable communication channels?*

Include the relevant procedure in which this is described in the information file and indicate below where this can be found in the information file (page numbers and paragraph(s)).

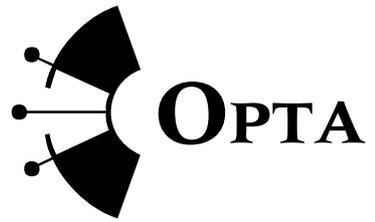
C.7 *What is the return policy in the event of liability?*

Include the relevant procedure(s) in which this is described in the information file and indicate below what this appendix is called and where it can be found in the information file (page numbers and paragraph(s)).

C.8 *How do you communicate any changes in the general conditions to the holders of qualified certificates and how do you register these holders' approval of the changes?*

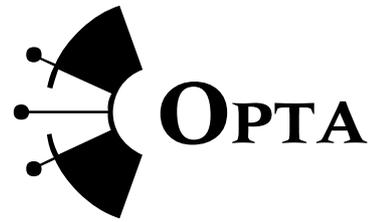
Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

**Certification service provider
offering qualified certificates**



- C.9 List all restrictions applied by your company regarding the use of certificates you have issued.*
Include the relevant procedure(s) in which this is described in the information file and indicate below what this appendix is called and where it can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



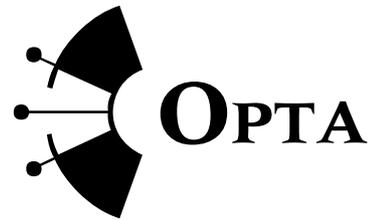
D Providing certification services in actual practice

D.1 Which activities does your organisation perform to reflect the reliability of your services with reference to qualified certificates? Complete the following list to indicate in which sections of the Certification Practice Statement (CPS) or any other documents your organisation has formulated the necessary rules and applications to promote the reliability.

Include the Certification Practice Statement and any other procedures referred to in the information file. Location of Certification Practice Statement CPS and any other additional procedures (including document names) in the information file:

Indicate where in the CPS or any other additional documents the following measures are covered:	Document name	Page	Paragr aph
1. <i>The procedures that describe the manner in which the requirements that are included in the Qualified Certificate policy (QCP) are covered.</i>			
2. <i>The obligations, including the applicable rules and applications, of all external organisations that support the certification services.</i>			
3. <i>Making the aspects of the Certification Practice Statement (CPS) and other relevant information needed to assess conformance with the Qualified Certification Policy(QCP) available to contract parties and certificate holders.</i>			
4. <i>Publicising the general conditions with reference to the use of qualified certificates for all contract parties, certificate holders and potential trusting parties.</i>			
5. <i>The certification service provider has a high management body that bears ultimate responsibility for the Certification Practice Statement (CPS) for the supply of qualified certificates.</i>			
6. <i>Higher management bears ultimate responsibility for correct execution of the Certification Practice Statement (CPS) for the supply of qualified certificates.</i>			
7. <i>The certification service provider has a process to periodically evaluate execution in practice, including the manner in which responsibility is borne, so that the Certification Practice Statement (CPS) continues to be satisfied.</i>			
8. <i>Timeous availability of proposed changes in the Certification Practice Statement (CPS) and, after approval by a body referred to in point 5, availability of the changed Certification Practice Statement (CPS) in the manner described under point 4.</i>			
9. <i>The certification service provider applies procedures and processes in the areas of administration and management in accordance with a described quality system that is in keeping with the latest developments in the area of quality systems. If you are certified for this, we request that you include this certificate in the information file.</i>			

Certification service provider offering qualified certificates



E Key management for qualified certificates

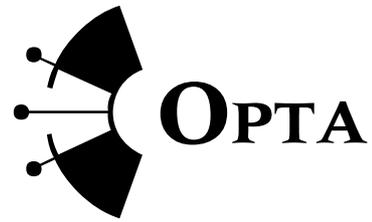
E.1 How does your organisation ensure that the correct procedures are applied in generating the keys that are used for the services provided and that the correct resources are used? Describe where your organisation has registered the use of the correct procedures and resources in the following table. Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragr aph
1. <i>Generation of keys by the certification service provider is done in a physically secured environment.</i>			
2. <i>Generation of keys by the certification service provider is only performed by representatives employed for this purpose.</i>			
3. <i>Generation of keys by the certification service provider is done under dual verification.</i>			
4. <i>Generation of keys by the certification service provider is done in a device that is suitable for this purpose.</i>			

E.2 In generating keys for the certification service provision, does your organisation ensure that this is done in a device that satisfies at least the requirements stated in FIPS 140-2 level 3 or higher, or CEN Workshop Agreement 14167-2 and/or 14167-1 or in a secured system that satisfies EAL 4 or higher qualification in accordance with ISO/IEC 15408, or similar security requirements? Include copies of the certificates of the devices used in the information file and indicate below what these certificates are called and where they can be found in the information file (page numbers and paragraph(s)).

E.3 What type of algorithm with which key length and what type of random generator are used to generate the certification service provision keys for the qualified certificates? Include a description of the relevant algorithms and key lengths used in the information file and indicate below what these algorithms are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



E.4 How does your organisation ensure that its private keys for the provision of certification services remain secret and intact? Indicate the procedures that safeguard this in the following table.

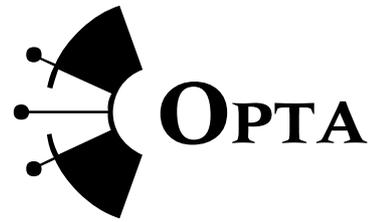
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. The private key for signing qualified certificates is used and stored in a device secured by means of cryptography.			
2. If the private key for signing qualified certificates is not in the secured device, it is encrypted. The algorithm used and the key length that is used for the encryption is excellent according to today's standards and can withstand crypto analysis attacks during at least the remainder of the life time of the encrypted private key or key part plus the maximum life time of the certificates issued with this private key.			
3. The tasks of making of back-ups, restoring and saving of private keys for signing qualified certificates are only executed by a minimum number of staff members employed for this purpose.			
4. The tasks of making of back-ups, restoring and saving of private keys for signing qualified certificates are executed under a protection level that, as a minimum, consists of dual verification.			
5. The tasks of making of back-ups, restoring and saving of private keys for signing qualified certificates are only executed in accordance with the certification service provider's instructions.			
6. If the private key for signing qualified certificates is stored in a dedicated module for generating keys, the access security ensures that this key cannot be accessed in this module from the outside.			

E.5 Does your organisation store and use the private key for signing qualified certificates in a device secured by cryptography that at least satisfies the requirements stated in FIPS 140-2 level 3 or higher, or CEN Workshop Agreement 14167-2, or in a secured system that satisfies EAL 4 or higher qualification, or similar security requirements?

Include copies of the certificates of the devices used in the information file and indicate below what these certificates are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



E.6 How does your organisation ensure the authentication and integrity in distributing the public key used and the relevant attributes for verification of qualified certificates issued, and how do you ensure that the origin of this information is known?

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

E.7 Indicate whether your organisation stores private keys in such a way that this information can be used later to unlock data that has been encrypted in some way (Key escrow), or emphatically does not do so. Indicate the procedure used to safeguard this.

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Yes, only private keys for signing qualified certificates:

Yes, only private keys of holders of qualified certificates:

Yes, both of the above types of private keys.

No, neither of the above types of private keys.

E.8 Are the private keys of the certification service provider for signing qualified certificates only used to generate qualified certificates? Include as appendix a procedure in which this is described.

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Yes, _____

No, _____

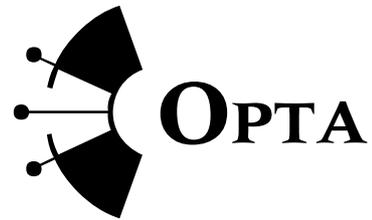
E.9 Are the private keys for signing qualified certificates only used on a physically secured area (both physically and logically)? Include as appendix a procedure in which this is described.

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Yes, _____

No, _____

Certification service provider offering qualified certificates



E.10 Which actions are taken at the end of the lifetime of the key pairs used in your process? Include as appendix a procedure in which this is described.

- Original private keys of the certification service provider and any copies thereof are destroyed in such a way that these private keys can no longer be identified. Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).
-

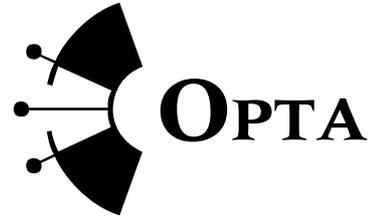
- Original private keys of the certification service provider and any copies thereof are filed in such a way that they are protected from re-use. Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).
-

E.11 In what way does your organisation secure the equipment used for signing qualified certificates during their entire life cycle? Indicate which necessary measures your organisation has safeguarded in which procedure in the following table.

Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>During transport of cryptographic equipment that is used to sign qualified certificates, the integrity is not compromised and no attempts are made to compromise the integrity.</i>			
2. <i>During storage of cryptographic equipment that is used to sign qualified certificates and lists with suspended and revoked certificates (CRL), the integrity is not compromised and no attempts are made to compromise the integrity.</i>			
3. <i>The operation of cryptographic equipment during installation, activation, saving of back-up copy/copies of private keys that are used to sign qualified certificates and retrieval thereof is done simultaneously by at least two staff members employed for this purpose.</i>			
4. <i>The cryptographic equipment used to sign qualified certificates and the list of suspended and revoked certificates (CRL) functions properly.</i>			
5. <i>The private keys used to place the signature of the certification service provider stored in cryptographic equipment are destroyed when the equipment is permanently taken out of operation.</i>			

Certification service provider offering qualified certificates



E.12 Does your organisation generate key pairs for certificate holders of qualified certificates?

- Not applicable.
- No
- Yes, complete the following table and indicate which procedure(s) safeguard this.
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file: _____

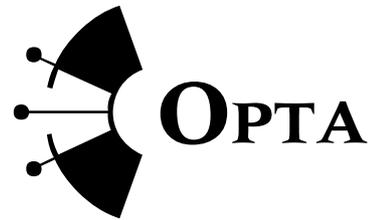
Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>The algorithm used and the key length used to generate key pairs for certificate holders of advanced electronic signatures</i>			
2. <i>The key pairs for certificate holders of qualified certificates generated by the certification service provider are securely generated and securely stored before they are delivered to the certificate holder.</i>			
3. <i>The private key of the certificate holder is delivered to the contract party or certificate holder in such a way that it cannot be compromised and only the certificate holder can gain access to his private key.</i>			

E.13 Is a secured device (SSCD) required to place an advanced signature?

- No
- Yes, complete the following table and indicate which procedure(s) safeguard this.
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file: _____

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>The preparations (personalisation) of the secured device (SSCD) takes place under control and under the supervision of the certification service provider.</i>			
2. <i>The secured device (SSCD) is stored and distributed securely.</i>			
3. <i>Switching the secured device (SSCD) on and off is done using information associated with the certificate holder (e.g. PIN code). This information is delivered securely to the certificate holder, separately from the secured device (SSCD).</i>			

Certification service provider offering qualified certificates



F Management of qualified certificates and public key infrastructure (PKI)

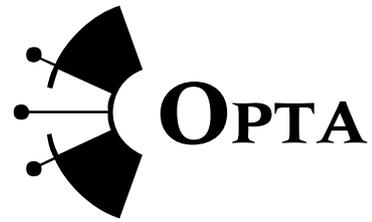
F.1 In what way does your organisation verify the identity and any specific attributes of the persons with whom an agreement is entered into within the framework of supplying qualified certificates? Give an exhaustive description of this and indicate which proof is requested (physical characteristics and documents), and which information is stored by you in the process.

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

F.2 The contract party need not by definition be the certificate holder. For example in commercial situations, the certification service provider may enter into an agreement with a legal entity. In that case, the certification service provider does not have an agreement with the certificate holder(s). In what way does your organisation verify the identity and any specific attributes of the persons with whom no agreement is entered into and who is related to a person with whom you have entered into an agreement? Give an exhaustive description of this and indicate which proof is requested (physical characteristics and documents), and which information is stored by you in the process.

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates

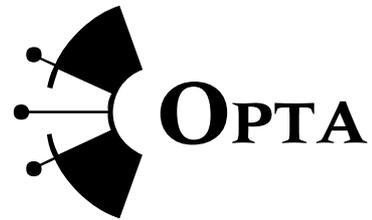


F.3 What information do you request during the application procedure and what information from the data received do you register? Answer the questions in the following table with yes or no.

1. Is the certificate holder of the qualified certificate required to give a home address or other contact data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Is all data used for verification of the identity of the certificate holder stored?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Are all restrictions regarding the validity of a qualified certificate stored?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Is the signed certificate holder agreement stored with the certificate holder?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the certificate holder agreement contain approval by the certificate holder of the certificate holder obligations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the certificate holder agreement contain, if applicable, approval by the certificate holder of mandatory use of a secured device (SSCD)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does the certificate holder agreement contain approval by the certificate holder of storage of his data as submitted upon application, delivery and where applicable revocation, and of possible transfer of this data under the same conditions to third parties upon termination of the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8. Does the certificate holder agreement contain an indication that the certificate holder approves publication of his certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9. Does the certificate holder agreement contain a statement by the certificate holder that all data in the certificate are correct?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10. Is all relevant data submitted upon application, delivery and possible revocation stored at least seven years after termination of the validity of the qualified certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
11. Is the certificate holder informed in writing of the storage period of at least seven years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12. Does the application procedure for a qualified certificate include verification of a certificate holder's possession of a private key generated by the certificate holder that is associated with the public key for which the qualified certificate is being requested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

F.4 Does your organisation deviate from the application process for new qualified certificates if a change in, or extension or revision of an existing qualified certificate is being requested while retaining the old key pair? Also indicate any deviations if only the key pair is to be revised. If so, describe these. Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



F.5 In what way does your organisation ensure that the certificates are issued in a secure manner in such a way that their authenticity is safeguarded and that the issue of qualified certificates is in keeping with the requirements specified in Section 3 of the Decision Requirements Certification Service Providers and Electronic Signatures? Answer the questions in the following table with yes or no.

1. Does the qualified certificate state that it was issued as a qualified certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does the qualified certificate state the identification and the country in which your organisation is established?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the qualified certificate state the name of the certificate holder or a pseudonym identified as such?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does the qualified certificate contain space for a specific attribute of the certificate holder that, if required, can be stated depending on the objective of this certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the qualified certificate contain the certificate holder's public key for verification of the certificate holder's signature?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the qualified certificate state the beginning and end dates of its validity?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does the certificate state the certificate's identity code?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8. Is the qualified certificate signed with your advanced electronic signature as certification service provider?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9. If applicable, does the qualified certificate state any restrictions on its use?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10. If applicable, does the qualified certificate contain limits regarding the value of transactions for which the certificate can be used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

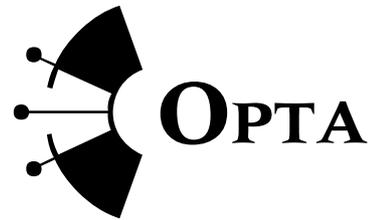
F.6 Do you always guarantee the uniqueness of the name that is assigned to a certificate holder in your domain? In other words, will it be impossible to use a name that has been used earlier for a different entity?

- Yes
 No

F.7 How do you monitor the integrity and confidentiality of the certificate holder's data or contract party data, in particular when transferring this data from the certification service provider to the contract party or certificate holder and between the various parts of the process?

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



F.8 *If you use external registration authorities, how do you verify that the exchange of registration data takes place with one of the official registration authorities whose identity has been determined?*

Include the relevant procedure(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

F.9 *In what way has your organisation organised the issue of qualified certificates and relevant information? Answer the questions regarding this procedure in the following table.*

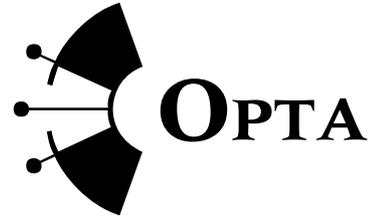
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>How does your organisation ensure after generation that the complete and correct qualified certificate is made available to the certificate holder for whom it is intended?</i>			
2. <i>How does your organisation ensure that the applicable general terms are immediately recognisable as such when a qualified certificate is issued?</i>			
3. <i>How does your organisation ensure that the general terms and qualified certificates for which approval has been given are publicly and internationally available 24 hours a day, 7 days a week?</i>			
4. <i>Which measures has your organisation taken to make this information public and internationally available within a foreseeable period of time in the event of a human or system error, as defined by your organisation in its Certification Practice Statement (CPS)?</i>			

F.10 *How do you ensure that qualified certificates are only supplied to third parties with approval from the certificate holder?*

Include the relevant list in which this is described in the information file and indicate below where this can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates

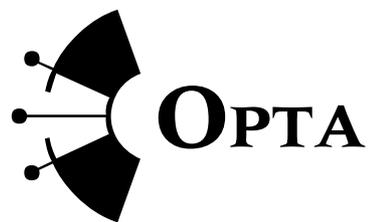


F.11 In what way has your organisation organised the process for revocation and suspension of qualified certificates? Answer the questions regarding these procedures in the following table.

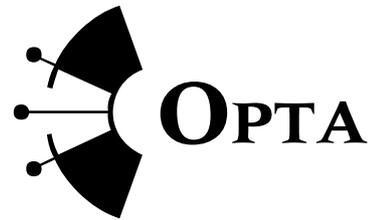
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file: _____

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. Who may request revocation reports and revocations? (part of Certification Practice Statement CPS)			
2. How are revocation reports and revocation requests applied for? (part of Certification Practice Statement CPS)			
3. Which requirements are applied to requests for revocation reports and revocations? (part of Certification Practice Statement CPS)			
4. For which reasons are qualified certificates suspended or revoked? (part of Certification Practice Statement CPS)			
5. In what way and for how long is the status of a revocation made available? (part of Certification Practice Statement CPS)			
6. What is the maximum delay between the time that a revocation request or revocation report is received and the status information is changed in the list with suspended and revoked qualified certificates (CRL) available to all? (maximum within 24 hours)			
7. How and when are requests for revocation or revocation reports due to reasons such as a compromised private key, the death of the certificate holder, violation of contract obligations and unexpected termination of a certificate holder agreement or operational functions processed?			
8. In what way are the identity, authenticity and authorisation of the source of a revocation request or revocation report verified? (part of Certification Practice Statement CPS)			
9. When is the status 'suspended' assigned to a qualified certificate and how long does the suspension remain applicable?			
10. How is the certificate holder and, if applicable, the contract party of a suspended or revoked qualified statement informed of a change in the status of the validity of its qualified certificate?			
11. How do you ensure that a revoked qualified certificate is not re-issued?			
12. With what frequency are the lists of suspended and revoked qualified certificates (CRL) published?			
13. How does your organisation ensure that every list of suspended and revoked qualified certificates (CRL) indicates when a new list will be published?			
14. Which 'trusted (issuing) third party' signs the list of suspended and revoked qualified certificates for you (CRL)?			
15. How do you ensure that revocation services are available 24 hours a day, 7 days a week?			
16. Which measures has your organisation taken to provide these revocation services within a foreseeable period of time in the event of a human or system error, as defined by your organisation in its Certification Practice Statement (CPS)?			
17. How does your organisation ensure that the list of suspended			

**Certification service provider
offering qualified certificates**



<i>and revoked qualified certificates (CRL) is publicly and internationally available 24 hours a day, 7 days a week?</i>			
18. <i>Which measures has your organisation taken to make the list of suspended and revoked qualified certificates publicly and internationally available within a foreseeable period of time in the event of a human or system error, as defined by your organisation in its Certification Practice Statement (CPS)?</i>			
19. <i>How does your organisation secure the integrity and authenticity of the information in the list of suspended and revoked certificates (CRL)?</i>			

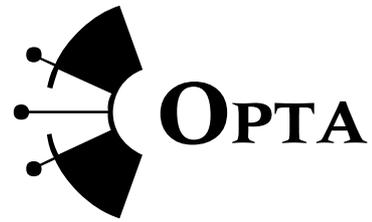


G Security and safeguarding of management and operations

G.1 How does your organisation ensure that adequate administrative and management procedures are applied that are in keeping with the accepted standards? Indicate whether your organisation has implemented procedures that achieve this obligation in the following table.
Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>The provider of qualified certificates retains ultimate responsibility for all aspects of the services provided, including when that provider uses third parties for certain functions. Indicate how this delegated responsibility is made known to these parties.</i>			
2. <i>Indicate the resources your organisation uses to ensure that third parties implement measures required by you in order to delegate part of the responsibility.</i>			
3. <i>Management must use a high-level forum to determine the policy for information security.</i>			
4. <i>The management is responsible for making the information security policy known to all employees that are involved in this policy.</i>			
5. <i>Every change in the infrastructure or the policy that affects the level of security is approved by a forum that is responsible for information security.</i>			
6. <i>Indicate where your organisation has registered the fact that a security plan in which the security procedures and work descriptions for the facilities, systems and information for the provision of qualified certificates is defined and maintained.</i>			
7. <i>How does your organisation ensure that the security plan is also implemented?</i>			
8. <i>The provider of qualified certificates safeguards the security of information when delegating responsibility for execution of certain functions to third parties.</i>			
10. <i>The certification service provider periodically performs a risk analysis to evaluate the necessary security requirements and the operational procedures.</i>			

Certification service provider offering qualified certificates



G.2 Where has your organisation registered the fact that it performs risk analyses to periodically evaluate operational risks and to determine the necessary security measures and procedures? Indicate how and where your organisation has registered in its security plan the risk analysis of all its information resources and the relevant security requirements; refer to the table of contents of the security plan that is to be included with this application as an appendix.

Include the table of contents of the security plan or other procedures in which this is described in the information file and indicate below where these can be found in the information file (page numbers and paragraphs).

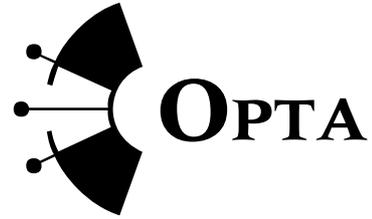
G.3 In what way do you ensure that the operational resources and information receive an adequate level of security? Indicate how and where your organisation has taken measures in its security plan in order to achieve this; refer to the table of contents of the security plan that is to be included with this application as an appendix.

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below where these can be found in the information file (page numbers and paragraphs).

G.4 Does your organisation maintain a list of the operational resources and information with the relevant security classifications that are in keeping with the risk analysis? Indicate how and where your organisation has taken measures in its security plan in order to achieve this; refer to the table of contents of the security plan that is to be included with this application as an appendix.

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below where these can be found in the information file (page numbers and paragraphs).

Certification service provider offering qualified certificates

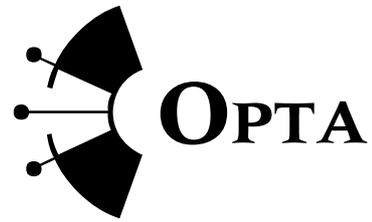


G.5 *In what way does your organisation ensure that its staffing policy supports and strengthens trust in the execution of the provision of services? Indicate how and where your organisation has taken measures in its security plan in order to achieve this; refer to the table of contents of the security plan that is to be included with this application as an appendix.*

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragr aph
1. <i>How has your organisation registered the fact that your personnel has the expertise, experience and qualifications necessary to provide qualified services that are in keeping with the task descriptions?</i>			
2. <i>How has your organisation registered the security roles and responsibilities?</i>			
3. <i>Where has your organisation registered the fact that it ensures that there are job descriptions that have been compiled from the perspective of:</i> <ul style="list-style-type: none"> • <i>division of positions,</i> • <i>preventing exceptions from occurring,</i> • <i>the sensitivity of a position based on tasks and access levels,</i> • <i>necessary background checks,</i> • <i>necessary training,</i> • <i>employee awareness.</i> <i>The job descriptions should preferably also describe the necessary skills and experience. Where possible, a differentiation is made between general positions and specific positions.</i>			
4. <i>Where is the fact registered that the personnel apply work descriptions and administrative and management procedures that are in keeping with the procedures and requirements as described in the security plan?</i>			
5. <i>Where is the fact registered that personnel with management responsibility are appointed on the basis of expertise in the area of advanced electronic signature technology and familiarity with security measures for personnel with security responsibility?</i>			
6. <i>Where is the fact registered that all personnel with confidential positions and/or tasks have no other activities or interests that (appear to) conflict with execution of the position or tasks?</i>			
7. <i>How has your organisation registered the defined confidential positions and/or tasks?</i>			
8. <i>Where has your organisation registered that personnel are assigned official responsibility for confidential tasks and by which representative these assignments are made?</i>			
9. <i>Where is the fact registered that your organisation does not allow confidential or management tasks to be performed by persons who have been convicted of a serious crime and/or who have committed any other crime that would make them less suitable for the relevant position?</i>			

Certification service provider offering qualified certificates

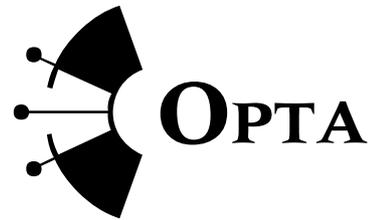


G.6 *In what way do you ensure that physical access to critical functions and services is controlled and that the physical risks for operational resources are minimised? Indicate how and where your organisation has taken measures in its security plan in order to achieve this; refer to the table of contents of the security plan that is to be included with this application as an appendix.*

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragr aph
1. <i>Indicate how the physical access to areas involved in certificate generation, issue of devices to certificate holders and management of the revocation of certificates is limited to authorised persons.</i>			
2. <i>Indicate where you have registered the measures you take to prevent loss, damages or compromising operational activities and interruption of the provision of services.</i>			
3. <i>Indicate where and which measures you have registered that you take to prevent compromising or theft of information and information-processing resources.</i>			
4. <i>Indicate where and which measures you have registered to physically protect the environment of the areas in which qualified certificates are generated, certificate holder devices are issued and revocation management occurs in order to protect it from being compromised by unauthorised access to systems and/or data.</i>			
5. <i>Indicate where your organisation has registered the fact that physical protection is to take place by means of clearly defined security perimeters (e.g. physical barriers) around the generation of qualified certificates, the issue of certificate holder devices and revocation management. Every part of the complex that is shared by other organisations is kept outside of these perimeters.</i>			
6. <i>Where in your security plan has your organisation registered the physical measures and security resources used to secure the areas in which the systems are located, the systems themselves and the operating rooms for these systems?</i>			
7. <i>Where in the security plan has your organisation included the physical measures and security resources for the generation of qualified certificates, the issue of certificate holder devices and revocation management that focus on unauthorised access, natural disasters, fire, gas, water and light malfunctions, danger of collapse, leaks, theft, burglary and dealing with calamities?</i>			
8. <i>Indicate where and which security measures your organisation has registered that it takes against unauthorised removal of equipment, media and software related to its provision of services.</i>			

**Certification service provider
offering qualified certificates**

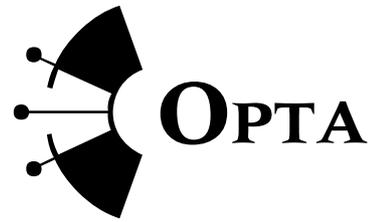


G.7 *Where has your organisation registered the fact that the systems are secure and operated properly with a minimal risk of errors, and the manner in which this is ensured? Indicate how and where your organisation has taken measures in its security plan in order to achieve this; refer to the table of contents of the security plan that is to be included with this application as an appendix.*

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragr aph
1. <i>Indicate where your organisation has registered how the systems and information are protected from viruses, software with which unauthorised actions are (or could be) taken, and unauthorised software.</i>			
2. <i>Indicate where your organisation has registered how damage due to security incidents and system shortcomings are minimised by using incident reporting and response procedures.</i>			
3. <i>Indicate where your organisation has registered how media is to be safely used to prevent damages to, theft of and unauthorised access to the media.</i>			
4. <i>Indicate where your organisation has registered which procedures are applied for all confidential and administrative positions that affect the provision of qualified certificates.</i>			
5. <i>Indicate how your organisation ensures that all media are used in accordance with the required classification scheme (see also G.2).</i>			
6. <i>Indicate how your organisation destroys media with confidential and/or sensitive data when it no longer needs to be saved.</i>			
7. <i>Indicate the methods applied by your organisation to ensure that sufficient processor time and storage capacity will be available in the future.</i>			
8. <i>Indicate how your organisation ensures that security incidents are responded to within a suitable period of time and in a coordinated manner.</i>			
9. <i>Indicate how fast security incidents are to be reported.</i>			
10. <i>Indicate how your organisation separates the security processes for qualified certificate services from the normal processes. In any event, this pertains to operational procedures and accounting, management of secured systems and acceptance of new secured systems, protection against enemy and/or unauthorised software, housekeeping, network management, active monitoring or audit reports, event analyses and responses, the application and security of media, and data and software exchange.</i>			

Certification service provider offering qualified certificates

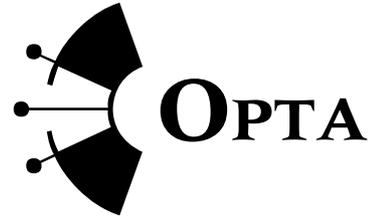


G.8 *In what way have you ensured that the systems are only accessible for authorised persons? Indicate how and where your organisation takes measures in its security plan to achieve this.*

Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>Indicate which measures your organisation has registered and applies, e.g. a firewall, to secure your internal network from access via third networks outside the domain for the provision of qualified services. Firewalls are also configured in such a way that these obstruct protocols and access requests that are not required for your provision of services.</i>			
2. <i>Indicate how your organisation secures confidential and/or sensitive data, including certificate holder information, if and when it is transported over non-secure networks..</i>			
3. <i>Indicate how your organisation applies effective administration of certificate holder access (operators, network administrators and other certificate holders with access to the system) to maintain system security.</i>			
4. <i>Indicate how your organisation limits access to information and system applications in keeping with the access policy.</i>			
5. <i>Indicate how your organisation uses sufficient computer security resources to safeguard the distinction between confidential functions, including the distinction between security and production functions, and in particular how systems and applications are protected and strictly controlled.</i>			
6. <i>Indicate how your organisation determines the identity and authenticity of personnel before they can use critical applications for the provision of qualified certificates.</i>			
7. <i>Indicate how your organisation holds the personnel liable for their activities.</i>			
8. <i>Indicate which measures your organisation takes to prevent perusal of sensitive and/or confidential information by unauthorised certificate holders by re-using storage capacity or by undeleting files that have been deleted.</i>			
9. <i>Indicate how your organisation ensures that local network elements such as routers, switches and hubs are placed in a physically secure environment and their configurations are audited regularly.</i>			
10. <i>Indicate how your organisation continuously guards against unauthorised and/or irregular behaviour to acquire access to the systems for the generation of qualified certificates and revocation management, and indicate which alarm facilities are used to detect such behaviour.</i>			
11. <i>Indicate how your organisation manages access to applications for the distribution of qualified certificates and lists of suspended or revoked qualified certificates (CRL) in such a way that attempts to delete or add qualified certificates or to modify information related to qualified certifications are prevented.</i>			

Certification service provider offering qualified certificates



- G.9** *How do you ensure that only reliable systems and products that are protected from modifications are used? Indicate how and where your organisation takes measures in its security plan to achieve this.*

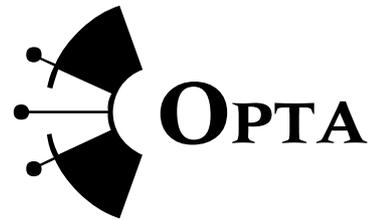
Refer to the table of contents of the security plan included earlier in the information file or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>Indicate how your organisation ensures that, in compiling functional specifications for a system to be developed or equipment to be purchased for the provision of qualified certification services, an analysis is made of the security requirements in order to ensure that security is built into the IT system.</i>			
2. <i>Indicate which procedures you apply for the installation of new releases, modifications and emergency solutions for operational software.</i>			

- G.10** *In what way do you ensure that the provision of services is restored as quickly as possible in the event of calamities, including the situation in which the private key for the certification signatures has been compromised? Submit the business continuity plan or the disaster recovery plan and answer the following questions.*

Refer to the business continuity plan or the disaster recovery plan or include other procedures in which this is described in the information file and indicate below what these procedures are called and where these can be found in the information file (page numbers and paragraphs).

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>Indicate where the fact is registered that it is considered a disaster if the private key of the advanced certification signature is compromised or if such is suspected.</i>			
2. <i>Indicate how quickly after the occurrence of a disaster the provision of services is restored.</i>			
3. <i>Indicate where your organisation has registered the activities it performs in the event that the private key used to issue qualified certificates is compromised.</i>			
4. <i>Indicate how your organisation deals with the certificates you issue and the revocation status list if the private key of a provider of qualified certificates with whom you cooperate is compromised.</i>			



H Termination of the supply of qualified certificates

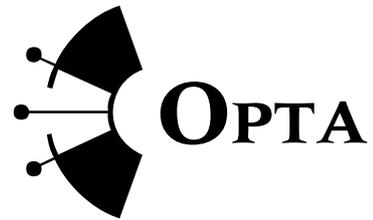
H.1 Which provision(s) has your organisation made to transfer the qualified certificates issued to another provider of qualified certificates upon termination or interruption of the provision of services?

Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

H.2 In what way does your organisation ensure that in the event that the supply is unexpectedly terminated or interrupted, potential problems that could ensue for the holders of qualified certificates and trusting parties are minimised? How is maintenance of files with information that could be used in legal procedures continued? Indicate which measures you take to achieve this in the following list of questions.

Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

Indicate the procedure in which the following measures are covered:	Document name	Page	Paragr aph
1. <i>Indicate where your organisation has registered how and when all holders of qualified certificates, known and unknown trusting parties and other providers of qualified certificates with whom you cooperate are informed of termination of the provision of services.</i>			
2. <i>Indicate when the qualified certificates still valid at that time are revoked.</i>			
3. <i>Indicate where your organisation has registered how permission for parties that perform tasks for your provision of services is withdrawn.</i>			
4. <i>Indicate where your organisation has registered how all obligations regarding the maintenance of certificate holder registration information and event files are transferred during the applicable legal periods and as told to certificate holders and trusting parties.</i>			
5. <i>Indicate where your organisation has registered how and when the private keys used for the provision of services are destroyed or revoked for further use.</i>			
6. <i>Indicate where your organisation has registered the arrangements made by you to reimburse costs involved with the termination, including in the event of bankruptcy.</i>			
7. <i>Indicate where the measures referred to above, in particular notification of affected entities, the transfer of obligations to other parties and dealing with the revocation status of certificates issued that are still valid, are included in the Certification Practice Statement (CPS).</i>			



I Data storage

I.1 In what way does your organisation store all relevant information pertaining to a qualified certificate during the period that the qualified certificate is valid and for a period of at least seven years after its validity has ended, in particular in the interest of evidence for legal procedures? This pertains in particular to five important types of information, i.e.: the qualified certificate, certificate holder registration data, significant information from the environment of your organisation, information regarding key management, and information about certificate management events. Indicate how you have registered the storage of this information in the following table.

Include the relevant procedure(s) in which this is described in the information file. Locations and names of these procedures in the information file:

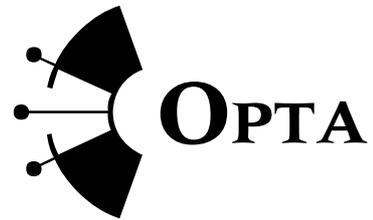
Indicate the procedure in which the following measures are covered:	Document name	Page	Paragraph
1. <i>Indicate where your organisation has registered which information is stored and what archiving methods are applied per type of information.</i>			
2. <i>Indicate where your organisation has registered how the reliability and integrity of your archives for your services that pertain to qualified certificates are maintained and which security methods are used in this respect.</i>			
3. <i>Indicate where your organisation has registered the fact that the data of holders of qualified certificates are completely and confidentially stored in accordance with the methods described in the Certification Practice Statement (CPS).</i>			
4. <i>Indicate where you have registered how long the various types of information are stored.</i>			
5. <i>Indicate where you have registered which event files are stored.</i>			

I.2 Does the holder of the qualified certificate have access to his certificate holder data as stored and other relevant personal data?

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

Certification service provider offering qualified certificates



I.3 *Does your organisation supply information regarding qualified certificates if this is requested for legal procedures?*

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

I.4 *Does your organisation store the exact time of events that pertain to key management, certificate management and the environment of the provision of certification services with an accuracy of at least one minute?*

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

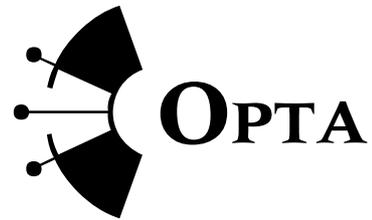
No: indicate below why not.

I.5 *Does your organisation store events in such a way that they cannot be easily deleted or destroyed during the period in which these files are stored?*

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

Certification service provider offering qualified certificates



I.6 Does your organisation store data regarding events involving registration, revision requests and re-key requests?

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

I.7 Which registration information is stored upon the issue of a qualified certificate? Answer the following questions with yes or no:

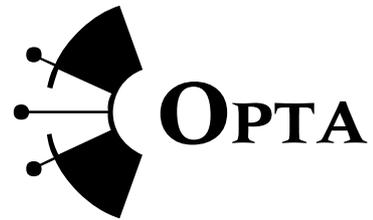
1. Does your organisation store documents or copies thereof that have been submitted with the application for a qualified certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does your organisation store identification data, numbers or a combination thereof if you require this information with an application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does your organisation store the storage location of the copies of applications, identification documents and signed certificate holder agreements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does your organisation store the specific choices made by the holder of a qualified certificate, e.g. publication of the qualified certificate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does your organisation store the identity of the person who accepts or approves the application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does your organisation store the method with which identification documents are validated where applicable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. If applicable, does your organisation also store the name of the receiving and/or requesting registration authorities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

I.8 Does your organisation store all events regarding the life cycle of your keys that are used to provide services that are related to qualified certificates?

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

Certification service provider offering qualified certificates



I.9 Does your organisation store events regarding the life cycle of qualified certificates issued?

Yes: how long? _____

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

I.10 Does your organisation store events regarding the life cycle of keys that you manage?

Yes: how long? _____

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

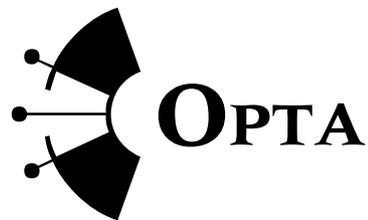
I.11 Does your organisation store events regarding the preparation of secured devices (SSCD), if you perform this activity (or have it performed)?

Yes: how long? _____

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

Certification service provider offering qualified certificates



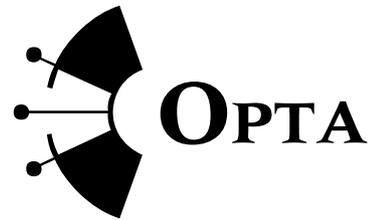
I.12 *Does your organisation store all requests and reports regarding revocation of qualified certificates as well as the results of such a request or report?*

Yes: how long? _____

Yes: indicate the name of the procedure and on which page(s) and paragraph(s) this is implemented and where this information can be found in the information file.

No: indicate below why not.

Certification service provider offering qualified certificates



J Trust in the organisation

J.1 How does your organisation ensure that policy and procedures are non-discriminatory? How, for example, do you deal with requests for a qualified certificate from an entity that is established in another country?

Include the relevant procedure(s) and/or description(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

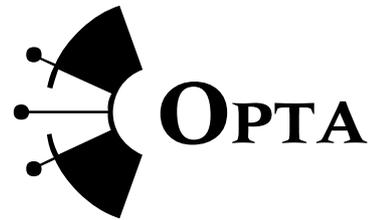
J.2 In what way does your company ensure that it is reliable? Indicate whether you have or have not achieved the items that promote trust in the following table. Separate, supporting information need not be included because the necessary supporting information is already present or is easily acquired by other means.

1. Are the services accessible for any applicant whose activities are in keeping with the target group of the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does your organisation use a system or multiple systems for quality and security management that is or are attuned to the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Is your organisation a legal entity that is established in keeping with corporate law in the Netherlands?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does your organisation have adequate measures to bear liability ensuing from the supply of the services, damages in particular?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Is your organisation financially stable and does it have access to the resources for providing the services in accordance with the regulations and the international standards applied by your organisation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does your organisation employ sufficient adequately trained and experienced personnel to offer the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does your organisation have a complaints and conflicts procedure for the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8. Does your organisation an adequately documented summary of contracts and agreements with third parties used for the provision of services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9. Does your organisation employ one or more executives or employees who, during the last five years, have been imposed a conditional or unconditional prison sentence for a period of more than six months?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

J.3 The provider of qualified certificate may not be known to have committed earlier crimes. Can you submit for each executive in your organisation and for each employee bearing responsibility for processing confidential or sensitive information within the framework of the provision of qualified certification services a statement of good behaviour (as issued by the municipality where the relevant executive or employee resides)?

Include the relevant statements in the information file and indicate below what these appendixes are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



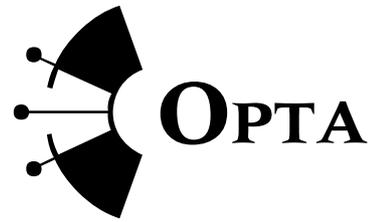
- J.4 *In what way does your organisation ensure that the parts that are responsible for management of the functions 'generation of qualified certificates' and 'revocation of qualified certificates' are independent of other parts of the organisation in the area of decision making regarding development, supply, maintenance and withdrawal of services? In particular, the chairman of the executive board, the senior staff and employees in confidential positions must be free of any commercial, financial or other interest that could influence the reliability of your provision of services in any way. Which measures, for example with reference to other positions, have been taken in this respect?*

Include the relevant procedure(s) and/or description(s) in which this is described in the information file and indicate below what these procedures are called and where they can be found in the information file (page numbers and paragraph(s)).

- J.5 *In what way has your organisation assigned the parts of the provision of services responsible for the generation and revocation of qualified certificates to a fixed position in the organisational structure that guarantees the independence of the execution? Indicate how you have achieved this.*

Include the relevant procedure(s) and/or description(s) in which this is reflected in the information file and indicate below what these appendixes are called and where they can be found in the information file (page numbers and paragraph(s)).

Certification service provider offering qualified certificates



K Signature

If you:

- have completed all questions (except if you are certified under the TTP.NL scheme; see also question B.2)
- **and** have described your public offer (manner in which, resources, target group) and included it in the information file
- **and** have included a valid excerpt from the registration in the trade register, the register of associations or the register of foundations not older than six months and a copy of your valid passport or European identification document in the information file
- **and** have included all requested documents in an orderly and accessible manner
you can sign this form.

The undersigned (name in block letters) _____

declares that the information has been completed correctly, fully and in truth and that he is familiar with the fact that rights and obligations of himself and others may change under the influence of changes in the European and/or national regulations. The undersigned also declares to have familiarised himself with the explanation to the registration form regarding the value that may or may not be assigned to a registration with OPTA. OPTA retains the right, in the event that a certification service provider assigns a different value to the registration in its external communication, to publicly add nuance.

City _____ date _____ signature _____

If your organisation has collective signature authority, place the signatures of other authorised representatives below:

The undersigned declare that the information has been completed correctly, fully and in truth and that they are familiar with the fact that rights and obligations of himself and others may change under the influence of changes in the European and/or national regulations. The undersigned also declare to have familiarised themselves with the explanation to the registration form regarding the value that may or may not be assigned to a registration with OPTA. OPTA retains the right, in the event that a certification service provider assigns a different value to the registration in its external communication, to publicly add nuance.

The undersigned (name in block letters) _____

City _____ date _____ signature _____

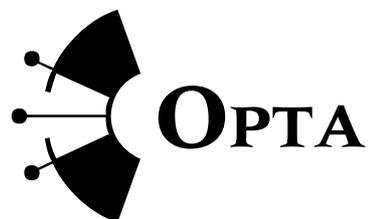
The undersigned (name in block letters) _____

City _____ date _____ signature _____

The undersigned (name in block letters) _____

City _____ date _____ signature _____

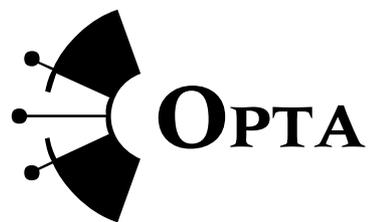
Bijlage bij het registratieformulier
**Aanbieder van Gekwalificeerde
certificaten aan het publiek**



**Cross-reference table application form, ETSI TS 101 456, Annex
II Electronic Signature Directive 1999/93/EC and General Ordinance Decision Requirements
Electronic Signatures**

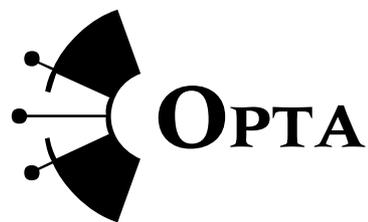
Application form	TS 101 456	Annex II	General Ordinance
A.1			
A.2			
A.3			
B.1	5.2a, 5.3.1b, 5.3.2c		
B.2			
B.3			
B.4	5.4.1, 5.4.1b		
B.5			
C.1	5.3, 5.3.1, 5.3.1b, 5.3.2, 5.4.1a		
C.2	5.2		
C.3	5.2, 5.2b, 7.3.4, 7.3.4a	k)	Sct. 2 sub-sct. q and u
C.4	6.2, 6.2a thru h, 7.3.4	k)	Sct. 2 sub-sct. q and u
C.5	5.4.1, 6.3, 6.3a thru c, 7.3.4	k)	Sct. 2 sub-sct. q and u
C.6	7.3.1a and b, 7.3.4b and 7.3.5c	d), g), k)	Sct. 2 sub-sct. j, Sct. 2 sub-sct. d and Sct. 2 sub-sct. q and u
C.7	6.4		
C.8	7.3.2b	d), g)	Sct. 2 sub-sct. j and Sct. 2 sub-sct. d
C.9	6.4		
D.1	7.1, 7.1a thru h	a)	Art 2 sub-sct. a, b, g, h and i
E.1	7.2.1a thru b	f)	Sct. 2 sub-sct. c
E.2	7.2.1b	f)	Sct. 2 sub-sct. c
E.3	7.2.1c and d	f)	Sct. 2 sub-sct. c
E.4	7.2.2, 7.2.2a thru e	f), g)	Sct. 2 sub-sct. c and Sct. 2 sub-sct. d
E.5	7.2.2a	f), g)	Sct. 2 sub-sct. c and Sct. 2 sub-sct. d
E.6	7.2.3, 7.2.3a	g), i), l)	Sct. 2 sub-sct. d, Sct. 2 sub-sct. l and Sct. 2 sub- sct. m
E.7	7.2.4		
E.8	7.2.5, 7.2.5a		
E.9	7.2.5, 7.2.5b		
E.10	7.2.6, 7.2.6a		
E.11	7.2.7, 7.2.7a thru e		
E.12	7.2.8, 7.2.8a thru d	f), g), j)	Sct. 2 sub-sct. c, Sct. 2 sub-sct. d and Sct. 2 sub-sct. p

Bijlage bij het registratieformulier
**Aanbieder van Gekwalificeerde
certificaten aan het publiek**



E.13	7.2.9, 7.2.9a thru d		
F.1	7.3.1c and d	d), g), k)	Sct. 2 sub-sct. j, Sct. 2 sub-sct. d and Sct. 2 sub-sct. q and u
F.2	7.3.1c and e	d), g), k)	Sct. 2 sub-sct. j, Sct. 2 sub-sct. d and Sct. 2 sub-sct. q and u
F.3	7.3.1f thru j	d), g), k)	Sct. 2 sub-sct. j, Sct. 2 sub-sct. d and Sct. 2 sub-sct. q and u
F.4	7.3.2, 7.3.2a, c, d	d), g)	Sct. 2 sub-sct. j and Sct. 2 sub-sct. d
F.5	7.3.3, 7.3.3a	g), Annex I 1999/93/E C	Sct. 3 sub-sct. a thru j
F.6	7.3.3d	g)	Sct. 2 sub-sct. d
F.7	7.3.3e	g)	Sct. 2 sub-sct. d
F.8	7.3.3f	g)	Sct. 2 sub-sct. d
F.9	7.3.5, 7.3.5a, d, e and f	b), l)	Sct. 2 sub-sct. n and o and Sct. 2 sub-sct. m
F.10	7.3.5b	b), l)	Sct. 2 sub-sct. n and o and Sct. 2 sub-sct. m
F.11	7.3.6, 7.3.6a thru k	b), l)	Sct. 2 sub-sct. n and o and Sct. 2 sub-sct. m
G.1	7.4.1, 7.4.1b thru f	e)	Sct. 2 sub-sct. b and f
G.2	7.4.1a, 7.4.2	e)	Sct. 2 sub-sct. b and f
G.3	7.4.1a, 7.4.2	e)	Sct. 2 sub-sct. b and f
G.4	7.4.1a, 7.4.2, 7.4.2a	e)	Sct. 2 sub-sct. b and f
G.5	7.4.3, 7.4.3a thru i	e)	Sct. 2 sub-sct. b and f
G.6	7.4.4, 7.4.4a thru g		
G.7	7.4.5, 7.4.5a thru h	e)	Sct. 2 sub-sct. b and f
G.8	7.4.6, 7.4.6a thru l	b), f), l)	Sct. 2 sub-sct. n and o, Sct. 2 sub-sct. c and Sct. 2 sub-sct. m
G.9	7.4.7, 7.4.7a thru b	f), l)	Sct. 2 sub-sct. c and Sct. 2 sub-sct. m
G.10	7.4.8, 7.4.8a thru b	a)	Art 2 sub-sct. a, b, g, h and i
H.1			Sct. 2 sub-sct. r and s
H.2	7.4.9, 7.4.9a thru c	a), i)	Art 2 sub-sct. a, b, g, h and i, Sct. 2 sub-sct. l, Sct. 2 sub-sct. s and Sct. 2 sub-sct. t
I.1	7.4.11, 7.4.11a, b, e and g	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.2	7.4.11c	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l

Bijlage bij het registratieformulier
**Aanbieder van Gekwalificeerde
 certificaten aan het publiek**



I.3	7.4.11c	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.4	7.4.11d	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.5	7.4.11f	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.6	7.4.11h	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.7	7.4.11i	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.8	7.4.11k	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.9	7.4.11l	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.10	7.4.11m	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.11	7.4.11n	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
I.12	7.4.11o	c), i)	Sct. 2 sub-sct. k and Sct. 2 sub-sct. l
J.1	7.5a	a)	Art 2 sub-sct. a, b, g, h and i
J.2	7.5, 7.5b thru i	a), h)	Art 2 sub-sct. a, b, g, h and i and Sct. 2 sub-sct. e
J.3			Sct. 2 sub-sct. g
J.4	7.5j	a)	Art 2 sub-sct. a, b, g, h and i
J.5	7.5k	a)	Art 2 sub-sct. a, b, g, h and i