TRUST SERVICES AGREEMENT FOR WEB SERVER SSL CERTIFICATES
NO. _____

I. CONTRACTING PARTIES

CERTSIGN S.A., with the registered office in Bucharest, 107A, Sos. Oltenitei, C1 building, 1st floor, office 16, sector 4, registered with the Trade register Office under no. J40/484/17.01.2006, Tax Identification Code RO18288250, bank account with IBAN RO90BRDE410SV91167344100 opened with BRD Calderon branch, hereinafter referred to as **certSIGN** or **Provider**, on one hand and

_____, with the registered office in Bucharest, str. _____, nr. ____, sector ___, identified in the Trade Register by the number _____, Tax Identification code RO with the bank account _____ opened with _____, legally represented by _____, as _____, hereinafter referred to as the **Beneficiary**, on the other hand.

II. DEFINITIONS

- **Certification Practice Statement of certSIGN Web CA (CPS)** - is the set of practices and procedures governing the provision and use of trust services for DV and OV server certificates, as applicable; depending on the type of certificate purchased, the CPS is available at the following addresses:
  - CPP SSL DV at https://www.certsign.ro/ro/document/certsign-web-ca-dv-cod-practici-si-proceduri/;
  - CPP SSL OV at https://www.certsign.ro/ro/document/certsign-web-ca-ov-cod-practici-si-proceduri/;
- **Terms and conditions for the provision of trust services for website authentication (T&C)** – are the terms and conditions relating to the provision of certification services for server certificates, in accordance with applicable laws, available at https://www.certsign.ro/ro/document/certsign-web-ca-termeni-si-conditii/;
- **Applicant** - the natural person empowered by the Subscriber to represent it in the relationship with certSIGN, to manage the certificates, to sign the T&C and to fulfil other formalities required for the issuance of SSL digital certificates.

III. SUBJECT MATTER OF AGREEMENT

3.1.   The subject matter of this agreement is the provision of trust services for an web server SSL certificate valid for 1 year in accordance with the provisions of EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market. („eIDAS"):

Purchased item*	Quantity** (pieces)	Unit price (EUR, VAT excluded)	Total price (EUR, VAT excluded)
☐ Services – DV SSL web server certificate (domain validation)		60	
☐ Services – OV SSL WEB server certificate (organisation validation)		150	
☐ Services – OV wildcard SSL web server certificate (organisation validation wildcard)		350	

* Select the service you want to purchase
** Enter the number of certificates you want to purchase

IV. DURATION OF AGREEMENT

4.1.   This agreement shall enter into force on the date of signature by both parties and shall be valid for a period of 1 year.

4.2.   The agreement may be extended through an addendum signed by both parties.

V. CONTRACTUAL VALUE. PAYMENT TERMS.

5.1.   The value of the contract is equal to the value of the services purchased.

5.2.   The price in EUR shall be paid in RON, at the exchange rate communicated by the NBR, valid on the date of invoicing, by payment order, to the account of the Provider mentioned in point I of this agreement, within 3 (three) working days from the date of invoicing via the RO-eFactura system.

5.3.   Invoices will be issued on the date the certificates are issued.

5.4.   If the Beneficiary fails to meet its payment obligation within the time limit laid down in the contract, the Provider shall be entitled to charge a penalty of 0.1% per day of delay of the amount of the outstanding debt.

VI. OBLIGATIONS OF THE PARTIES

6.1.   Obligations of the Beneficiary

The Beneficiary undertakes:

6.1.1. To comply with the provisions of this contract;

6.1.2. To take note and comply with the provisions of this contract, the T&C and the CPS and, both he and the Applicant, use the certificates and any other services provided by certSIGN only in accordance with their provisions and applicable law;

6.1.3. To pay for the services covered by this contract under the conditions and within the time limits laid down herein;

6.1.4. The applicant designated by the Beneficiary to represent it in the relation with certSIGN is:

Ord. no.	Last name / First name of Applicant	E-mail of Applicant	Telephone
1			

6.1.5. To provide certSIGN with accurate and complete data and inform the Applicant about the transmission of its data to certSIGN for the provision of the services covered by this contract;

6.1.6. By signing this contract he acknowledges and agrees that the data in the certificate will be made available to the public by publishing the certificate in the Certificate Repository immediately after certSIGN issues it, for the purpose of providing the service;

6.1.7. To take the necessary measures to ensure: i) the generation by the Beneficiary of the cryptographic request(s) required for the issuance of the requested certificates, ii) the proper generation and secure storage of the private key within a key pair (to prevent its loss, compromise, modification and unauthorized use) and iii) the control, confidentiality, and protection of the private key corresponding to the public key to be included in the certificate requested by the Applicant;

6.1.8. To use the digital certificate issued by the CERTSIGN WEB CA Certification Authority:

- OID 1.3.6.1.4.1.25017.3.1.4.5 Certificate for Website Authentication - with Domain Validation (DV SSL)
- OID 1.3.6.1.4.1.25017.3.1.4.2 Certificate for website authentication - with Organisation Validation (OV SSL)

as appropriate, in accordance with the scopes and restrictions established by the CPS;

6.1.9. To check the information included in the certificate for accuracy;

6.1.10. To install the Certificate only on servers that are accessible to the subjectAltName listed in the Certificate and use the Certificate in accordance with applicable law and the CPS and only for the purposes stated in the Certificate and in accordance with;

6.1.11.   To notify certSIGN of any changes to the information on the basis of which the certificates purchased by the Beneficiary have been issued, as soon as possible after they occur;

6.1.12.   To immediately request the revocation of the certificate and cease the use of the certificate and its associated private key if it identifies any actual or suspected misuse or compromise of the Applicant's private key associated with the public key included in the certificate or as soon as the essential information contained in the certificate no longer corresponds to the reality. The request shall state the reasons for revocation in accordance with the Mozilla Root Store Policy requirements, described in Appendix 2;

6.1.13.   The Beneficiary understands and agrees that certSIGN has the right to revoke the certificate immediately if the Applicant violates the T&C or if certSIGN discovers that the certificate is being used for illicit activities, such as phishing attacks, fraud or malware distribution;

6.1.14.   The Beneficiary understands and accepts that the revocation of the Certificate for any of the reasons mentioned above or for non-payment of the price under the conditions laid down in the contract does not lead to the refund of the price or to a free re-issue of the Certificate.

6.1.15.   To transmit to certSIGN the documentation required for the issuance of the certificate within 5 days from the date of signature of this agreement. The Beneficiary shall submit the following documents:

> ➢ purchase order on the model in Annex no.1;
> ➢ copy of the identity document of the Applicant designated in accordance with point 6.1.4 herein, signed and dated by the Applicant;
> ➢ T&C completed and signed by the Applicant
> ➢ in the case of OV SSL server certificates and OV wildcard SSL certificates, in addition to the documents mentioned above, also provide:
>   - certificate of status not older than 30 days;
>   - proof of representation of the person signing the agreement.

Also, for issuance it will be necessary to submit the SSL Web Certificate (.csr) application electronically to customer@certsign.ro.

6.1.16.   By signing this agreement he acknowledges that certSIGN will keep a copy of the Applicant's identity document for the purpose of processing the information required exclusively for the issuance of the digital certificate.

Any failure by the Beneficiary/Applicant to comply with its obligations under this contract, the T&C and the CPS shall be considered a breach of this contract.

6.2.   Obligations of certSIGN

Certsign undertakes:

6.2.1. To provide the SSL Web server certificate within 5 days from the date of receipt from the Beneficiary of the complete documentation required for the issuance of the certificate;

6.2.2. certSIGN will issue the SSL certificate only after having validated the request and verified the documents and data transmitted by the Beneficiary in accordance with the CPS;

6.2.3. To comply with the European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as well as national implementing legislation, in relation to the services provided;

6.2.4. To comply with the provisions of this contract, the T&C and the CPS;

6.2.5. To ensure the security of its own IT systems used for the provision of trust services, using industry-recognised practices recommended by applicable standards;

6.2.6. certSIGN is bound to revoke any certificate in accordance with the CPS. certSIGN will immediately inform the Beneficiary/Applicant of the revocation of the certificate together with the reasons for its decision to the email address of the Applicant. certSIGN will enter the revocation of the certificate in the Certificate Repository.

6.2.7. To ensure access to all information necessary for the correct and safe use of its services throughout the duration of this agreement;

6.2.8. Maintain the confidentiality of the information entrusted in the performance of this contract.
6.2.9. In case the keys of the Certification Authority that issued the certificate get compromised, certSIGN is bound to revoke the certificate(s) in accordance with the CPS.

VII. CERTIFICATE ACCEPTANCE

7.1.   Upon receipt of a certificate, the Beneficiary through the Applicant undertakes to verify its content, in particular the correctness of the data and the complementarity of the public key with the private key it holds. If the certificate shows irregularities, mistakes or any other discrepancy with the data submitted for registration, the Beneficiary through the Applicant shall immediately refer the matter to the Certification Authority with a view to revoking the certificate. The certificate shall be deemed accepted if the Applicant accepts it either explicitly, at the time of its retrieval from the certSIGN website, or implicitly, after 3 calendar days from the date of receipt of the certificate (sent by certSIGN).

7.2.   Acceptance of the certificate is a unilateral decision of the Beneficiary, prior to its use in any cryptographic operation.

VIII. CONTRACTUAL LIABILITY

8.1.   In the event of non-performance or improper performance of any of the undertaken contractual obligations, the injured party shall be entitled to claim damages from the party at fault, to the amount of the direct and pecuniary damage created and proven.

8.2.   By way of exception from the foregoing paragraph, certSIGN shall not be liable in any way for damages caused by loss of control or confidentiality of the private key of the certificate, unauthorised use of the certificates or for any negligence of the Beneficiary/Applicant in their safekeeping and use or if the data submitted by the Beneficiary and/or the Applicant are false, inaccurate, incomplete or outdated or if false identity documents are submitted. It shall also not be liable for damages incurred by the Beneficiary or third parties caused by the use by the Applicant of certificates issued by certSIGN.

8.3.   To the extent permitted by law, neither party shall be liable to pay damages for consequential loss, lost profit or benefit, loss of business, loss of customers or loss of data.

8.4.   The Provider's liability for an SSL Web server certificate shall be limited to the value of the certificate.

8.5.   In the event of contract termination for non-fulfilment of contractual obligations due to the fault of the Beneficiary, certSIGN shall revoke all operational certificates subject to this agreement.

IX. CONFIDENTIALITY

9.1.   "Confidential Information" means any data and/or information, regardless of their nature, disclosed directly and/or indirectly by one Party to the other during the term of the Agreement, as well as the data and/or information of which the Parties become aware and/or to which they have access during/as a result of the performance of this Agreement, including parts and/or copies (including copies of the Parties) of the data and/or information and/or derivatives thereof, regardless of how the data and/or information was disclosed (in writing, verbally, by electronic transmission of data or by any other means), regardless of the medium in/on which the data and/or information are contained and regardless of whether it is specified as confidential or not.

9.2.   The Parties undertake to use the Confidential Information only for the purpose of fulfilling the obligations undertaken under this Agreement (hereinafter referred to as the "Purpose") and to protect and keep such Confidential Information as strictly confidential.

9.3.   The Parties undertake, throughout the duration of the Agreement and after its termination, for a period of 5 years (hereinafter referred to as the confidentiality period), not to disclose and not to transmit, in any form and by any means, directly or indirectly, for any reason, to any third party the Confidential Information, not to sell and/or assign them, not to use them in the relationship with third parties, not to use them directly or indirectly, for their own benefit of for the benefit of a third party, and not to allow any third party access to Confidential Information.

certSIGN S.A.
VAT Code: RO18288250, Trade Register: J40/484/2006, Registered Capital: 2,095,560 LEI
Registered Office: 107A Oltenitei Avenue, C1 Building, 1st Floor, Room 16, S4, Bucharest, Romania
Telephone: +40 311011870, Fax: +40 21 311 99 05, E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806; ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Pag. 4 / 10
Contract WEB SSL
v2.4-feb.2024
Public

9.4.   The Party receiving the information undertakes, during the period of confidentiality, to disclose the Confidential Information only to the employees who are involved in the achievement of the Purpose and only as much as is necessary for the fulfilment of the Purpose. The Receiving Party undertakes that the Employees sign confidentiality commitments that provide at least the same degree of protection of Confidential Information as this Chapter.

9.5.   The Receiving Party is responsible for ensuring the security of confidential information both in terms of the means used for this purpose and the facts and acts of its employees, servants, collaborators and representatives and for any breach of these obligations by them.

9.6.   Confidential Information shall not be considered as public information only because certain characteristics, components and/or different combinations related thereto are and/or become public.

9.7.   The Receiving Party has no right, of any kind, to the Confidential Information, except the right to use such Confidential Information for fulfilling the Purpose and no provision of the Agreement and/or any other document shall be construed as transmitting or conferring any right on the Receiving Party with respect to the Confidential Information.

9.8.   Failure to comply with this obligation by a Party entitles the other Party to terminate the contract and to request the payment of damages at the value of the directly created and proven patrimonial damage.

X. PROCESSING OF PERSONAL DATA

10.1.   Each Party, when disclosing to the other Party personal data regarding its employees/representatives for the purpose of negotiating, concluding and executing the Agreement (the "Purpose"), shall ensure that it shall only disclose the information necessary for this purpose.

10.2.   Each Party shall request from the other Party only the personal data required to execute the contract and, insofar as there is another purpose for which it requests the personal data, it will justify this request by providing the information required by the applicable law, respectively by art. 13-14 of Regulation no. 679/2016 and / or any article or rule replacing or supplementing these provisions.

10.3.   Employees/representatives of the Beneficiary can find information about the processing of personal data carried out by the Provider for the achievement of the Purpose in the document "Privacy Policy", available at la https://www.certsign.ro/ro/politica-de-confidentialitate/.

10.4.   Personal data belonging to the Applicant shall be processed by the Provider in accordance with the Information Note on the processing of personal data available at https://www.certsign.ro/ro/nota-de-informare-gdpr-pentru-servicii-de-incredere/.

10.5.   Each Party disclosing personal data of its employees/representatives for the fulfilment of the Purpose shall make sure that it has provided them with the information set out in Articles 13-14 of Regulation 679/2016 and/or any article or rule replacing or supplementing these provisions.

10.6.   For the avoidance of doubt, the Parties acknowledge and agree that each Party shall independently determine the purposes and means of processing personal data in connection with this contract.

10.7.   Each Party independently undertakes responsibility for processing of personal data for achieving the Purpose. Violation, by a Party, of the provisions of this act, as well as of the provisions of Regulation no. 679/2016 and of the general mandatory norms adopted in relation to the protection of personal data, cannot be considered as a common infringement and cannot generate joint and several liability towards the person or the authority that finds this violation.

XI. CANCELATION

11.1.   Failure to comply with the obligations undertaken under this contract by one of the parties gives the injured party the right to request the lawful termination of this contract, without any other legal formality, other than the 30 days prior notification, and to claim the payment of damages to fully cover the created and proven damage.

11.2.   If the notified party performs its obligations or proves the initiation of enforcement measures within the 30-day period referred to in Article 11.1, the termination shall no longer apply.

11.3.   In the case referred to in Article 11.1, the party who has requested the termination of the contract shall only be entitled to claim payment in respect of the part of the contract performed up to the date of the actual termination of the contract.

XII.   TERMINATION OF AGREEMENT

12.1.   This Subscriber Agreement lawfully terminates, with no other legal formality, under the following circumstances:
- by reaching the term;
- by agreement of the parties;
- by contract cancellation, according to art. 11;
- one of the parties goes into foreclosure, judicial reorganization, bankruptcy or the operating permits are withdrawn;
- force majeure and or act of God, under the conditions of art. 13.

12.2.   Termination of agreement, in any of the situations mentioned in art. 12.1. will have no effect on the obligations already due between the parties.

XIII.   FORCE MAJEURE. ACT OF GOD

13.1.   The parties of this agreement shall not be liable for the failure to execute in due time and / or properly, in whole or in part, any of the obligations incumbent upon them under this agreement, if the failure to perform the said obligation was the result of a case of force majeure or Act of God.

13.2.   Force majeure refers to an unpredictable or unavoidable event produced after the conclusion of this agreement.

13.3.   An Act of God refers to a relatively unpredictable and invincible circumstance, of not an extraordinary nature, such as: strikes, legal restrictions, other such events.

13.4.   The party invoking any of the aforementioned events is required to notify the other party within 15 (fifteen) days of its occurrence and to prove it subsequently by supporting documents issued by the competent authorities.

13.5.   The contracting party that was prevented from performing its obligations due to those stipulated in art 13.2. and 13.3. will continue to perform its obligations after the termination of that event.

13.6.   If the events mentioned under art. 13.2. and 13.3. last for more than 2 (two) months, this agreement is considered lawfully terminated, without any further formalities being required.

13.7.   Cases of force majeure and Acts of God exonerate the contracting parties from the fulfilment of obligations undertaken herein, throughout the entire period they apply.

XIV.   WARRANTY OF COMPLIANCE

a) For the professional customer

The Provider offers a warranty of compliance for the services purchased throughout their provision period. The warranty period starts from the date of the digital certificate delivery, i.e. from the date on which the Beneficiary is able to access or use the digital certificate, even if it has not started using it. The warranty period offered is 12 months.

b) For the consumer customer

The Services covered by this Agreement are compliant with the compliance requirements set out in Geo 141/2021 on certain aspects relating to contracts for the supply of digital content and digital services.

Thus, these services meet the following compliance requirements:

- complies with the description, quantity and quality, including in terms of functionality, compatibility, interoperability, accessibility, continuity and security or any other characteristic provided for in the contract or normal for services of the same type and which the consumer can reasonably expect;

- correspond to the purpose for which the consumer requests them, known and accepted by the Provider, as well as to the purposes for a normal use of digital services of the same type, taking into account, as the case may be, the legal provisions or the applicable standards;
- are delivered with all the accessories, provided for in the agreement and which the consumer can reasonably expect;
- are supplied with updates in accordance with the contract and which the consumer can reasonably expect to have;
- are provided in the most recent version available at the time of conclusion of the agreement;
- are compliant throughout their period of performance;

However, certSIGN is not liable for the non-conformity of the services with the statements provided above under the conditions provided in art. 7 par. (2), (4) and (6) of GEO 141/2021.

The consumer has the right to invoke the legal warranty of compliance if a lack of conformity occurs within a period of one (1) year from the time the service is provided. The consumer must cooperate with the Supplier to the extent reasonably possible and necessary to establish if the non-compliance was caused by was caused by the consumer's digital environment.

The legal warranty of compliance entitles the consumer to have the service brought into conformity within a reasonable period of time, not exceeding 15 calendar days from the date of the request, without cost or major inconvenience to the consumer. The consumer shall be entitled to either a proportionate reduction of the price by continuing to use the service, or he may terminate the contract and obtain, as the case may be, a full refund or a share of the price paid, corresponding to the period of non-compliance, in exchange for giving up the service, if:

  i)   the provider fails or refuses to bring the service into conformity,
  ii)   the non-compliance is so serious that it justifies the immediate reduction of the price or the termination of the contract,
  iii) the service is not yet in conformity, despite the failure of the trader to bring it into conformity, or
  iv)   the bringing into conformity is impossible or disproportionate.

In the event of agreement termination, the consumer shall no longer be entitled to use the service. In cases where the lack of conformity is minor, the consumer shall have the right to terminate the contract only if it does not provide for the payment of a price.

XV. COPYRIGHT. INTELLECTUAL PROPERTY

15.1.   Copyright and related rights in technical documentation, services and products resulting from individual activities carried out by each Party shall remain the property of the Party that developed them and may only be used with its written consent.

15.2.   All copyright and related intellectual property rights in products, services, applications, designs, specifications, diagrams, models, industrial designs, logic diagrams, technological process diagrams, computer programs, names, trademarks, logos, promotional materials, etc. belonging to one of the Parties and used in the performance of the subject matter of the contract shall remain the property of that Party and shall not be subject to any transfer between the Parties and may only be used with the written consent of the Party owning them.

15.3.   The Beneficiary shall not be entitled nor shall it permit any other person to decompile, disassemble, reverse engineer or otherwise reconstruct the source code or the technology, methodologies or algorithms underlying the certSIGN Services and shall not cause or permit any other person to:

-    enter, even unintentional, viruses, Trojan horses, worms, "logic bombs" or other material that would in any way adversely affect the use of the certSIGN Services;
-    bypass, disable, in any form, any security features of the certSIGN system;
-    upload data, content that the Beneficiary does not own or have the right to use or that otherwise infringes the rights of individuals, copyrights, trademarks or other rights of third parties;
-    use any automated systems, including, but not limited to, 'bots', 'robots', 'web spiders' or

certSIGN S.A.
VAT Code: **RO18288250**, Trade Register: **J40/484/2006**, Registered Capital: **2,095,560 LEI**
Registered Office: 107A Oltenitei Avenue, C1 Building, 1ˢᵗ Floor, Room 16, S4, Bucharest, Romania
Telephone: +40 311011870, Fax: +40 21 311 99 05, E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806; ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Pag. 7 / 10
Contract WEB SSL
v2.4-feb.2024
Public

'offline readers' to access certSIGN systems in a manner that results in more request messages being sent to certSIGN systems than a human could reasonably have produced in the same period of time;

15.4. The Beneficiary shall defend and indemnify certSIGN for any infringements of intellectual property rights and copyrights, including infringements of the rights of third parties whose software is used in the management of the services, in case of breach of any of the obligations set out above, the limitations of liability in art. 8 not being applicable.

XVI.   OTHER PROVISIONS

16.1.   Contract amendment. Any amendment to this contract may only be made with the written consent of the two contracting parties, in the form of an addendum signed by both parties.

16.2.   Any communication between the parties relating to the performance of this contract must be in writing. Any written document must be recorded both at the time of transmission and at the time of receipt. Communications between the parties may be made by telephone or e-mail to office@certsign.ro,   subject to written confirmation of receipt of the communication at the addresses in the contract.

16.3.   Governing law. This agreement is subject to the provisions of Romanian law in force at the time of its conclusion and signing, and shall be amended and supplemented, where necessary, with the changes of the applicable legislation in the field, subsequently intervened.

16.4.   Jurisdiction. The parties mutually agree that all disagreements that cannot be settled amicably shall be submitted for settlement to the competent courts of Romania.

16.5.   All the documents constituted as annexes to this contract are an integral part thereof, completing and / or explaining certain clauses of the contract. The documents annexed to this agreement are:
  ➢   Annex no 1 – WEB SSL certificate purchase order
  ➢   Annex no 2 – Reasons for the WEB SSL certificate revocation

This agreement was drawn up today,_____, in two original copies, one for each signing party.

PROVIDER   **BENEFICIARY**

certSIGN S.A.
VAT Code: **RO18288250**, Trade Register: **J40/484/2006**, Registered Capital: **2,095,560 LEI**
Registered Office: 107A Oltenitei Avenue, C1 Building, 1ˢᵗ Floor, Room 16, S4, Bucharest, Romania
Telephone: +40 311011870, Fax: +40 21 311 99 05, E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806; ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Pag. 8 / 10
Contract WEB SSL
v2.4-feb.2024
Public

Annex no 1

WEB SSL certificate purchase order

The undersigned[1],……………………….., apply for the issue of a SSL certificate, for web servers of the following types and having the following addresses:

DNS	Server type:

To be filled in for the purchase of **DV SSL server** certificates

Mandatory fields	
Common Name	
Country	

To be filled in for the purchase of **SSL OV or OV wildcard** certificates

Mandatory fields	
Common Name	
Organisation	
Locality	
Country	

Beneficiary's signature

---

[1] Applicant

Annex no. 2
Reasons for the WEB SSL certificate revocation

No reason provided or unspecified (RFC 5280 CRLReason # 0) If the reason does not apply to the request for revocation, the Subscriber MUST not provide a reason code other than "***unspecified***" and the reason for revocation (CRLReason) will not be published.
KeyCompromise (RFC 5280 CRLReason # 1) The Subscriber MUST choose the reason for the revocation of "***keyCompromise***" when he has reason to believe that the private key of his certificate has been compromised, e.g. an unauthorized person had access to the private key of his certificate.
AffiliationChanged (RFC 5280 CRLReason # 3) The Subscriber should choose the reason for revoking ***"affiliationChanged***" when the name of the organisation or other organisational information in the certificate has changed.
Superseded (RFC 5280 CRLReason # 4) The Subscriber should choose the reason for the ***"superseded"*** revocation when requesting a new certificate to replace the existing certificate.
CessationOfOperation (RFC 5280 CRLReason # 5) The subscriber should choose the reason for revoking ***"cessationOfOperation"*** when he/she no longer owns all the domain names in the certificate or when he/she will no longer use the certificate because he/she interrupts his/her website.