Applies to:
OIDs: 1.3.6.1.4.1.25017.10.1.1; 1.3.6.1.4.1.25017.10.2.1; 1.3.6.1.4.1.25017.10.3.1; 1.3.6.1.4.1.25017.10.3.2; 1.3.6.1.4.1.25017.110.3.3

TERMS AND CONDITIONS
regarding the provision of trust services for Website Authentication

This deed is a contract, under article 1270 of the Romanian Civil Code, between:
certSIGN S.A., with the registered office in Romania, Bucharest, Oltenitei str. nr.107, building C1, 1st floor, office 16, Sector 4, registered with the National Trade Register under no. J2006000484402, Tax Identification Code RO18288250 as Trust Service Provider under the conditions set out in Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, hereinafter referred to as "certSIGN" and the **Subscriber** purchasing digital certificates for website authentication.
By signing/accepting these Terms and Conditions you agree to the terms and conditions for the provision and use of digital certificates for website authentication issued by certSIGN S.A., described as follows.

Purpose of Agreement
Submitting a certificate request to the certSIGN Registration Authority, or to a Registration Authority affiliated to certSIGN, for the issuance of a digital certificate implies accepting these Terms and Conditions described as follows. The provision of certification services by certSIGN shall be in accordance with the Certification Practice Statement of certSIGN Web CA G4, which is considered an integral part of these General Terms and Conditions.
certSIGN policies are validated by annual audit in accordance with the LSTI-Q055 certification scheme for Trust Service providers.

1. Definitions

"Subscriber" is the Legal Entity to whom a certificate is issued under a contractual relationship with certSIGN ("Agreement");
"**General Conditions**" refers this document "TERMS AND CONDITIONS regarding the provision of trust services for Web sites authentication".
"**Trust Services**" refer to the issuance, revocation, storage and verification of certificate status via http protocol using CRL and OCSP, verification of chain of trust (hierarchy) related to certificates for website authentication issued by certSIGN Web CA.
"Subject" device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
"Certification Practice Statement of certSIGN Web CA G4" (CPS) is the set of practices and procedures governing the provision and use of trust services for DV, OV, EV or QWAC server certificates, as applicable; the CPS is available at the following addreses: https://www.certsign.ro/en/document/certsign-web-ca-g4-certification-practice-statement/
Designated person: an individual designated by the Subcriber who applies for a certificate on behalf of the Subscriber; a legal representative or an employee of the Subscriber or an agent authorised to represent him: (i) who submits or approves a certificate request on behalf of the Subscriber and/or (ii) who signs a Subscriber Agreement or who accepts/acknowledges/signs these General Conditions on behalf of the Subscriber.
Other technical terms shall have the meaning assigned to them in the CPS, in ETSI EN 319411-1 and in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates available at https://cabforum.org/baseline-requirements-documents/.

2. Subject matter

It lays down the terms and conditions regarding the use and provision of trust services for Web sites authentication.

3. Duration

3.1 The contract enters into force upon the signing/acceptance of these General Conditions by the Subscriber.
3.2 These General Conditions are valid for the entire period of validity of the certificate purchased.

4. Obligations of the Subscriber

The Subscriber undertakes:
4.1 To provide certSIGN and/or the Registration Authority with correct and complete data for the purpose of issuing the certificate(s);
4.2. To take the necessary measures to enable the proper generation and secure storage of the private key within a key pair (to prevent its loss, compromise, alteration and unauthorised use);
4.3. To use the digital certificate issued by the Certification Authority certSIGN Web CA G4 according to the type of certificate purchased:

- OID 1.3.6.1.4.1.25017.10.1.1 Domain Validated Website Authentication Certificate (DV SSL)
- OID 1.3.6.1.4.1.25017.10.2.1 Organization Validated Website Authentication Certificate (OV SSL)
- OID 1.3.6.1.4.1.25017.10.3.1 Extended Validation Website Authentication Certificate (EV SSL)
- OID 1.3.6.1.4.1.25017.10.3.2 Qualified Website Authentication Certificate (QWAC SSL)
- OID 1.3.6.1.4.1.25017.10.3.3 Qualified Website Authentication Certificate for payment service providers in accordance with the EU Directive/PSD2 (QWAC SSL PSD2)

as applied,and in accordance with the scopes and restrictions established by the CPS
4.4. To check the information included in the certificate for accuracy;
4.5. To install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with the applicable law and the CPS and only for the purposes stated in the certificate. Intermediate authority certificates must be installed on the servers on which the server certificate is installed.
4.6. Immediately request certSIGN to revoke the certificate in accordance with Article 6 below, and to cease using it and its associated private key, if any actual or suspected misuse or compromise of the Subject's private key associated with the public key included in the certificate is identified;
4.7. To request certSIGN to revoke the certificate as soon as the essential information included in the certificate no longer corresponds to reality;
4.8. The Subscriber and the designated person understand and agree that certSIGN has the right to revoke the certificate immediately if they or any of them violate the provisions of these General Terms and Conditions or if certSIGN discovers that the certificate is being used for illicit activities, such as phishing, fraud or malware distribution.
4.9 By signing these General Conditions understands that certSIGN in order to issue the OV SSL digital certificate must verify the identity of the Subscriber;
4.10 By signing these General Conditions understands that certSIGN in order to issue the EV or QWAC SSL digital certificate must verify both the identity of the Subscriber and the Designated Person.
4.11. By signing these Terms and conditions the Subscriber consents to the publication of the certificate in the Repository immediately after issuance by certSIGN.
4.12. By signing these General Conditions, the Designated person acknowledges that certSIGN will keep a copy of his identity document in order to process the information necessary solely for providing the trust services.
Any failure by the Subscriber or the Designated person to fulfil the obligations will be considered a breach of General Conditions herein.

5. Obligations of certSIGN

certSIGN undertakes:
5.1 To comply with the CPS.
5.2 To issue the digital certificate within 5 (five) working days from the date of cumulative fulfilment of the following conditions, depending on the type of digital certificate purchased:
a) The Subscriber/Designated person has signed/accepted, as applicable, these General Conditions,
b) certSIGN has received in electronic format the SSL Web Certificate (.csr) application, together with the accompanying documents according to the type of certificate applied for, according to the CPS,
c) certSIGN has validated the request and the information received in accordance with the CPS applicable to the type of certificate requested,
d) domain and/or organisation validation has taken place, where applicable, by the methods established/requested by certSIGN according to the CPS,
e) for OV, EV or QWAC SSL certificates, the identity of the Subscriber has been verified
e) for the EV or QWAC SSL certificate, the identity of the Designated person has been verified,
5.3. To ensure the security of his own information systems used for providing trust services, using the practices widely recognized in the field and recommended by international standards,
5.4 If the key of the Certification Authority that issued the certificate is compromised, certSIGN shall revoke the certificate (s) according to CPS.

6. Certificate acceptance

Acceptance of certificates. Upon receipt of a certificate, the Designated person/Subscriber 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, errors or any other discrepancy with the data submitted for registration, the Designated person/Subscriber shall immediately refer the matter to the Certification Authority with a view to revoking the certificate. The certificate shall be deemed to be accepted 3 calendar days after the date of transmission of the certificate by certSIGN. Acceptance of the certificate is a unilateral decision of the Designated Person/Subscriber prior to its use in any cryptographic operation.

7. Revocation. Effects of revocation

7.1 The reasons which may lead to the revocation of the certificate shall be as follows:
- No reason provided or unspecified

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

The subscriber MUST select "keyCompromise" as the reason for the revocation 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

The Subscriber should choose "affiliationChanged" as the reason for revoking when the name of the organization or other organizational information in the certificate has changed.

- Superseded

The Subscriber should select " superseded " as the reason for revocation when applying for a new certificate to replace the expired one.

- CessationOfOperation

The subscriber should select "cessationOfOperation" as the reason for revoking when he no longer owns all the domain names within the certificate or when he will no longer use the certificate because of website interruption.

7.2 Revocation of the digital certificate, for whatever reason, will not result in a refund of the price or a free re-issue, but will result in termination of the service.

7.3 After revocation of the digital certificate for any reason, the Subscriber/Designated Person will no longer have the right to use it.

8. Confidentiality. Processing of personal data

8.1 "Confidential Information" means any data and / or information, regardless of its nature, disclosed directly and / or indirectly by the Subscriber/Subscriber's representative to the Provider during the performance of these General Conditions, 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 execution of these General Conditions, regardless of the medium in / on which the data and / or information are contained / transmitted and regardless of whether it is specified that they are confidential.

8.2 The parties undertake to use Confidential Information only for the purpose of fulfilling their obligations under these General Conditions, to protect it and to keep it confidential.

8.3 certSIGN will be exempted from liability for the disclosure of confidential information if one or more of the following conditions are met:

- the information was legally known and without a disclosure ban before it was received from the Subscriber
- the information has been disclosed after obtaining the Subscriber's written consent for such disclosure;
- certSIGN was legally bound to disclose the information.

8.4 certSIGN processes personal data in accordance with the provisions of REGULATION (EU) No 910/2014, EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("GDPR") and other applicable provisions of the Union or national law relating to data protection.

8.5 For the purpose of providing trust services, certSIGN processes personal data in accordance with the Notice on the Processing of Personal Data available at: https://www.certsign.ro/ro/nota-de-informare-gdpr-pentru-servicii-de-incredere/.

8.6 As a data subject, the Designated person has the rights set out in Articles 13 - 22 of the GDPR.

8.7 In order to manifest their rights with regard to their personal data, the data subject may contact certSIGN Personal Data Protection Department at the following contact details:

- email address: dpd@certsign.ro
- mailing address: 29A, Tudor Vladimirescu Bvd. AFI Tech Park 1, 2nd floor, Bucharest, sector 5

9. Cessation of Applicability

9.1 The present General Conditions shall cease to be applicable in the following situations:

a) upon certificate expiry;

b) upon certificate revocation;

c) upon the rejection of the certificate request;

d) upon non-acceptance of the certificate by the Subscriber/Designated person.

e) within 30 days of receipt of a notification from certSIGN, regarding the breach of obligations by the Subscriber/Subscriber's representative, if such breach, although possible, is not remedied within this period.

If remediation is not possible termination will take place with the communication of the notice.

10. Liability and Exceptions

10.1 certSIGN may be held liable under the conditions and within the limits laid down in the applicable law, in the current General Terms and Conditions, and in the contract.

10.2 certSIGN is not liable for:

a) the damages caused by force majeure and/or act of God. The term "force majeure" refers to that unpredictable and un-removable event that occurred after the Subscriber agreement was concluded, such as: fire, earthquake, any other natural calamity, as well as war. The relatively unpredictable and relatively invincible circumstance, with no extraordinary character, such as: strikes, legal restrictions, other such events, defines the act of God;

b) damages caused by installing and using applications and devices used for the generation and management of cryptographic keys, encryption, which do not meet the requirements specified in CPS;

c) damages caused by improper use of issued certificates ("improper" means the use of a revoked, or expired certificate inconsistent with the stated purpose of the certificate), the storage of erroneous data in certSIGN's databases and their

inclusion in digital certificates issued to the Subject, where the Subcriber/Designated person has declared such data to be correct.
d) submission by the Subscriber/ Designated person of false, inaccurate or incomplete data or of false documents, identity documents or statements. The Subscriber shall be solely liable for any damage suffered by certSIGN and third parties due to inaccurate and/or false information and documents submitted.
10.3 To the extent permitted by law, neither party may be bound to pay damages for consequential damages, or benefit or profit, loss of business, clients or data.
10.4 In any situation where certSIGN liability is incurred, it will be limited to the value of the EV or QWAC SSL server certificate. The total liability of the Provider shall not exceed USD 2,000 per certificate to cover damages caused regardless of the number of persons affected.

11. Governing law and dispute resolution

11.1. The Romanian law shall apply to the interpretation and enforcement of these General Terms and Conditions.
11.2. Any dispute arising from these General Terms and Conditions shall be settled by the competent courts of Romania.

12. Communications

12.1 Any communication between parties, referring to the execution of the contract, shall be transmitted in writing either by mailing and courier services or by e-mail at office@certsign.ro.
Any written document must be recorded both at the time of transmission and at the time of receipt.

13. Modification of the General Conditions

certSIGN reserves the right to amend these General Terms and Conditions when the amendment is required by legislation or standards applicable to the Trust Services or as a result of service improvements, or at the request of the competent authorities. The modification of these General Conditions will be published on the website www.certsign.ro and will be applicable from the date of publication.

PROVIDER
certSIGN S.A.

SUBJECT