TERMS AND CONDITIONS FOR CERTIFICATES FOR ELECTRONIC SEALS

Global Trusted Sign

Document Reference | FO24_GTS_V6
1 Terms and Conditions for the Use of Qualified Certificates issued by GTS

Global Trusted Sign (hereinafter referred to as GTS), in its condition of qualified trust service provider, offers diverse online services for digital products.

The use of services is subject to the following terms and conditions, being this document an agreement with the certificate subscriber and holder.

2 Qualified Trust Services

These terms and conditions apply to the use of qualified certificates for electronic seals issued by GTS.

By using these services, the holder understands that a qualified digital signature is equivalent to a handwritten signature, thus giving it probative value in the countries of the European Union, as well as in other countries that have declared the acceptance of Regulation (EU) 910/2014.

The user must read each document before proceeding to its qualified signature, when using these services.

The user accepts to notify GTS, as well as all relaying parties, in case his/her electronic mail changes, in order to ensure required conditions for the use of the services.

The user declares that, in the case of qualified certificates of professional type, he/she will inform GTS without delay when ceasing to exercise the professional competences established in the acquired certificate.

The holder also declares that he/she understands that printed copies of documents with qualified signatures do not have the same legal value of those digitally stored by the service.

3 Data Protection and Storage

To receive a Certificate for Electronic Seal, users must fulfill a certificate for electronic seal issuing form, where personal information, considered as sensitive, is required.

In the context of the GDPR in force, stored data in the remote server (HSM), must comply a set of protection requirements, to guarantee information privacy and security to holders.

In this regard, GTS declares that all data request and collection derive from the need to ensure electronic identification security means, to avoid identity misuse.
<table>
<thead>
<tr>
<th>Time Limits for the Storage of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information requested during the registration</strong></td>
</tr>
<tr>
<td><strong>From the selection of the service to the due payment</strong></td>
</tr>
<tr>
<td><strong>From the payment to the identity validation via videoconference</strong></td>
</tr>
<tr>
<td><strong>From the videoconference to the issuance of the certificate for Electronic Seals</strong></td>
</tr>
<tr>
<td><strong>Period of inactivity</strong></td>
</tr>
<tr>
<td><strong>Time limit for the right to data portability</strong></td>
</tr>
<tr>
<td><strong>Time limit for exercising the right to be forgotten</strong></td>
</tr>
</tbody>
</table>
4 Use restrictions

Certificates for electronic seals issued by GTS are used by different holders, systems, applications, mechanisms and protocols with the aim to allow the probative signature of documents by natural or legal persons, in accordance with provisions set forth in Regulation (EU) 910/2014.

The subscriber undertakes to comply with the terms and conditions herein, in accordance with the GTS Certification Practice Statement and Certification Policies (available at https://pki.globaltrustedsign.com/index.html) as well as with all the applicable legislation.

The subscriber is committed not to use the service for any unlawful purpose, not to provoke the interruption of the service, not to distribute contents that may breach the privacy, third parties' intellectual property rights or other related property rights, or for any other purpose that may be considered by GTS as unlawful, obscene, defamatory, fraudulent, abusive, threatening, prejudicial or objectionable.

The subscriber assumes responsibility for the content of all transactions made through the service.

5 Subscriber rights

In accordance with the General Data Protection Regulation in force, and its national implementation, all subscribers have rights over their data, i.e. the right to access (Art. 15); to rectification (Art. 16); to object (Art. 21); to restriction of processing (Art. 18); to data portability (Art. 20); or to the erasure of personal data (Art. 17), by contacting GTS. Furthermore, GTS is obliged to communicate all subscribers of its services that their data has been modified, erased or restricted of processing (Art. 19).

Also, GTS subscribers have the following rights: to lodge a complaint with a supervisory authority – in Portugal, the National Commission for Data Protection or CNPD, by its acronym in Portuguese- (Art. 77); to an effective judicial remedy against a supervisory authority (Art. 78); to an effective judicial remedy against a controller or processor (Art. 79); and to compensation and liability (Art. 82).

6 Subscriber obligations

The obligations of the subscriber / holder (including their representatives and agents) are:

1. To enforce the terms and conditions set forth in this document, as well as all specific conditions among the parties described in the contract;
2. To limit and to adequate the use of certificates in accordance with the GTS Certification Practice Statement and Certification Policies (available at https://pki.globaltrustedsign.com/index.html) as well as with all the applicable legislation;

3. Not to monitor, to manipulate or to perform “reverse engineering” activities on the technical implementation (hardware and software) of the certification services, without the prior written authorization of GTS;

4. To supply to GTS all information considered as accurate and complete related to any information that GTS may request for the registration process. Any modification of that data must be informed to GTS CA;

5. To verify that the private key used to sign is valid (i.e., it is not compromised) for the reception of the issued certificate;

6. In the event of knowledge of any unlawful behavior or access violation involving the qualified certificate, he/she shall notify GTS within a maximum period of 24 hours;

7. Use the Certificate, or the powers of representation, exclusively for the purposes for which the certificate was issued.

8. Inform GTS about all the documentation that has expired and make available the new updated documentation, provided that the holder intends to renew his/her certificate in the context of a simplified renewal.

9. Comply with security procedures, as well as all the technical requirements that have been established by GTS.

10. Request to GTS the immediate revocation of the Certificate, when there are suspicions of breach of confidentiality or when verified any of the reasons for revocation mentioned in the Certification Practice Statement, following the revocation procedure provided by GTS.

6.1. Qualified Digital Certificate Issuance Process

Before the issuance of the qualified certificate by the holder, the GTS CA must verify the identity of the subscribers and holders and, and, if applicable, other attributes of the holder, through the collection of direct evidence or proofs from appropriate and authorized sources, in accordance with the provisions of Article 24 of EU Regulation No. 910/2014, as regards compliance with the “requirements for qualified trust service providers”, particularly the following: “when issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued”.

For this, GTS has procedures “to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means”. The verification of the identity of the subscribers and/or holders will be carried out by the Administrators Working Group, and can be conducted in the following ways:
• In person, always with the presence in this act of two registry administrators (letter a, No. 1, Art. 24 of Reg. 910/014);
• Remotely, using electronic identification means, such as videoconferencing, through a certified software for this purpose, to which the presence of the natural person or of an authorized representative of the legal entity has been ensured, before issuing the qualified certificate, and in compliance with the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’ and Decision No. 154/2017 of the National Security Office (Gabinete Nacional de Segurança – GNS), (letter b, No. 1, Art. 24 of Reg. 910/2014; or
• By means of a certificate of qualified electronic signature or of qualified electronic seal, issued in accordance with the preceding paragraph (letter c and d, No. 1, Art. 24, of Reg. 910/2014), only for holders of Portuguese identity cards.

In case of choosing the videoconference, you should take into account the following:

I. The videoconference is scheduled after:

a) The respective payment is done;

b) The submission of requested documents;

c) The confirmation and validation of all data by the registry managers

II. Before starting the videoconference, it must be checked that all technical requirements are met and all documentation is available:

d) Verify your antivirus restrictions, since some antivirus do not allow to carry out a videoconference.

e) Use recommended browsers for the videoconference, such as Google Chrome or Firefox.

f) It is required to add a mobile network number, since during the validation of your identity, you will receive an activation code in your mobile.

g) The videoconference must be carried out in an illuminated area to allow the verification of the identity card (for instance, the hologram).

h) It is required to use a webcam and a microphone of acceptable quality level.

i) The videoconference can be done through a mobile phone with camera and microphone.

j) Check that you have your identity card and the mobile phone whose number was used to buy the qualified signature.

k) After the validation of your identity, in-situ or through a videoconference, you will have 30 approximately days to issue your qualified signature. Otherwise, you will have to repeat all the process.
I) If technical requirements are not met and if it is necessary to carry out a second videoconference, its cost will be charged to the client.

m) In these two last scenarios, €10,00 will be charged to carry out a new videoconference,

The videoconference is recorded for reasons of information protection. Consent is requested before starting the recording. In case this consent is not given, the validation must be conducted in person in one of the places that GTS facilitates for that effect.

III. When the validation of the holder identity is conducted through videoconference, the holder must submit the subscription forms by postal mail, if they are not digitally signed.

IV. The certificate issuance process concludes on the date of receipt by Global Trusted Sign of the Certificate Issuance Form duly completed and signed by the holder. GTS will conclude the process in a maximum of 2 business days, after receiving the documentation.

6.2. CDs Renewal

If the Holder wants to renew his/her certificate, and if the functions for which that certificate was issued are maintained, he/she must only request the renewal of the certificate with the same data and make the payment of the renewal following the indications that will be sent by GTS.

6.3. CDs Revocation

When a revocation request is verified, its execution will be carried out within a maximum period of 24 hours.

7 Amendments to the Certificate Issuance Form

If during the period of validity of the form, a new legislation, or a new regulation on the existing legislation is promulgated, related to issues included in these General Terms and Conditions and that produces changes in the fundamental obligations of the parties, and, if GTS also considers necessary to modify the terms of the Certification Practice Statement and the Qualified Certificates Policy established and/or contracted, these Terms and Conditions must be amended accordingly.

GTS will notify the holder about the contractual modifications, and its acceptance must be communicated by the holder within 30 days of such communication.

---

1 Lisbon, Porto, Ribeira Brava (Madeira) and Ponta Delgada (The Azores).
If the holder informs GTS the non-acceptance of the proposed amendments and being not possible to reach an agreement, any of the parties will be entitled to terminate this issuance form, and that denounce will take effects sixty days after the communication to the other party.

8 GTS obligations

The Trust Service Provider, as responsible entity for processing the holder data, is committed to ensure through its mechanisms, principles of fairness, loyalty, transparency, minimization, preservation limitation, proportionality, accuracy, safety and liability.

9 Obligations limits

GTS is responsible for damages or losses caused to final users and relying parties arising from its activity, according to the applicable legislation.

GTS is not responsible for other damages or losses derived from abusive use or those uses outside the scope of the contract with users and/or relying parties.

GTS is not responsible for the failure of services related to cases of force majeure, such as natural disasters, war or similar events.

GTS reserves the right not to conclude a purchase process for qualified digital certificates, when verified that the holder does not meet the requirements for the appropriate validation of the holder identity, being the applicant duly notified of the reasons.

The refusal to conclude the process, as long as it results from a cause not attributable to GTS, does not grant the holder the right to reimbursement of the amounts.

In particular, the holder will not be entitled to reimbursement of the amount paid for the certificate, if it is confirmed that he/she has provided false or incorrect information, or has omitted relevant information or documentation for the evaluation of the request, which is strictly necessary to continue with the process.

10 Use of the service

The holder of a public key certificate is only entitled to use the private key for the intended purposes (mentioned in the KeyUsage certificate field) within the law. The issuance and use of the certificate are always responsibility of its holder.
The use of the certificate is only permitted, and when applicable according the type of certificate:

- To whom is mentioned in the **Subject** certificate field;
- While the certificate is still valid and is not included in the Certificate Revocation List (CRL) of the certification authority of GTS. This list is available at [https://pki.globaltrustedsign.com/index.html](https://pki.globaltrustedsign.com/index.html) and in the properties of the certificate as demanded by the applicable legislation.

11 **Sharing information with Third Parties**

GTS is entitled to share information with competent authorities, when:

- It is obliged to do so by a subpoena, court order or any other judicial procedure of similar nature;
- It is necessary to comply with the legislation in force.

GTS subcontracts: PayPayUE – *Instituição de Pagamento, Unipessoal, Lda* – for the processing of payments via ATM, credit/debit card and MBWAY; iGEST platform for invoicing; and to qualified electronic signature and timestamps services, Identity Trust Management AG for videoconferences of validation of the identity of the holders, which is duly certified to operate in eIDAS Trust Service Providers.

12 **Preservation of audit records**

Audit records are preserved during the periods of time required by law, it means for 7 years.

13 **Availability of services**

CRLs can be checked at [https://pki.globaltrustedsign.com](https://pki.globaltrustedsign.com), ensuring its availability 24 hours a day, 7 days a week, except in cases of any programmed maintenance stoppage, duly informed to the parties involved.

Furthermore, revocation requests will be processed in 24 hours. During that time interval, the identity and authenticity of the person who requested the certificate revocation will be verified. After confirming the identity and authenticity of the requester, GTS has 60 minutes to change the certificate status to revoked.

Revoked certificates can be checked in the CRL of the Certification Authority of GTS.

GLOBAL TRUSTED SIGN does not guarantee the uninterrupted operation of the technological infrastructure that supports services mentioned in the Digital Certificate Issuance Form, in particular, when the infrastructure is subject to updates and improvements, required for the compatibility of GTS.
with possible legal or regulatory amendments, or with view to improve the complete operation of the infrastructure.

14 Compensations


15 Contacts

All stakeholders must use appropriate collective communications means. These means can include a digitally signed electronic mail, fax, signed forms or similar, depending on the severity and on the subject.

Telephone calls are recorded for purposes of quality control, with the due authorisation of the National Commission for Data Protection (Comissão Nacional de Proteção de Dados - CNPD). If you do not want your calls to be recorded, it is suggested to use alternative means.

<table>
<thead>
<tr>
<th>Name</th>
<th>GTS Management Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>ACIN-iCloud Solutions, Lda</td>
</tr>
<tr>
<td></td>
<td>Global Trusted Sign</td>
</tr>
<tr>
<td></td>
<td>Estrada Regional 104 Nº42-A</td>
</tr>
<tr>
<td></td>
<td>9350-203 Ribeira Brava</td>
</tr>
<tr>
<td></td>
<td>Madeira</td>
</tr>
<tr>
<td></td>
<td>Portugal</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:info@globaltrustedsign.com">info@globaltrustedsign.com</a></td>
</tr>
<tr>
<td>Website</td>
<td><a href="https://www.globaltrustedsign.com">https://www.globaltrustedsign.com</a></td>
</tr>
<tr>
<td>Telephone</td>
<td>707 451 451</td>
</tr>
</tbody>
</table>

16 Contact of the Data Protection Officer

In case of any doubt or any event related to data protection, GTS users may contact the Data Protection Officer (DPO – Art. 37, GDPR), appointed by the ACIN managers. This officer is available to provide support GTS clients and to cooperate with the appointed national supervisory authority – National Commission for Data Protection (Comissão Nacional de Proteção de Dados – CNPD). This officer can be contacted by e-mail dpo@acin.pt or telephone 707 451 451.
17 Dispute Settlement Provisions

Complaints must be sent to the GTS Management Group, via registered mail.

The Portuguese law is applied when any dispute arises from the interpretation or implementation of this document. The parties choose exclusively the legal jurisdiction of the District of Funchal to settle such disputes.

Any dispute between users and GTS can be communicated to the Supervising Authority, with the aim to settle any dispute that eventually may arise.

18 Applicable Legislation

The following legislation applies to certification authorities providing trust services:


b) Other national and European legislation related to activities of provision of qualified trust services;


Conformity audits will be regularly performed in GTS, pursuant the applicable legislation, by an external entity duly registered and acknowledged for that purpose, based on existing related provisions and its conclusions will be transmitted to the Supervising Authority, which can make publicly known the conclusions of all the process, when requested.

I hereby declare that I have understood the content of these Terms and Conditions:

___________________/_____ , _______________ , ________.

____________________________________________________________

(Signature)