TERMS AND CONDITIONS OF THE QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Global Trusted Sign

Document Reference | FO24_GTS_V10

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

The holder 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 holder 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.

Time Limits for the Storage of Information	
Information requested during the registration	At the time of registration, information regarding the name, surname, phone contact, email, TIN, country and desired password, is requested. This information is stored during 180 consecutive days from the registration date. After that period, and if the client does not express interest to buy any of GTS available products, that information will be deleted.
From the selection of the service to the due payment	The information required to acquire a service will be stored during 180 consecutive days. In case of no payment, all that information will be deleted. If after that period the holder intends to subscribe to the platform and to acquire a service, he/she must submit a new registration request.
From the payment to the identity validation	Once the payment has been made, the natural or legal person will receive a notification to schedule a videoconference for identity validation (Decision No. 154/2017 of the National Security Office - *Gabinete Nacional de Segurança* - GNS). In case the holder or his/her representative does not contact GTS to perform this validation in a period of 180 days from the date of the email reception, he/she will receive a new videoconference request in the next 7 days. In case the data validation is not carried out within the deadlines, all data will be deleted
From the identity validation to the issuance of the certificate for electronic seals	Once GTS has confirmed the identity of the legal or natural person, the holder must issue the certificate in a period of 180 consecutive days. If not, the holder will receive an email notifying that he/she must proceed to issue the certificate in the next 15 days. Otherwise, all data will be deleted. If it is necessary to repeat the videoconference, due to failure to generate the certificate within the requested period, it will be necessary to reschedule, with an additional payment of 10 euros (+ VAT at the current rate).
Period of inactivity	If an account that has been inactive for 9 months, GTS will notify the legal person/natural person/user, that in 180 business days must log in, otherwise, the account will be deleted.

Time limit for the right to data portability	GTS declares that in a maximum period of 180 days will execute any request related to the right to data portability submitted by a legal or natural person.
Time limit for exercising the right to be forgotten	To comply with legal provisions, not all information can be completely deleted, as the legal validity of qualified certificates must be preserved for extended periods of time, being defined by the CA as 7 years, pursuant to paragraph 1º, article 34º and recital 61 of Regulation (EU) 910/2014. Therefore, when the holder requests the right to be forgotten, only registration data will be deleted, but identity validation data of the holder and the certificate private key will be duly encrypted and preserved for 7 years. After that period, all data will be automatically deleted.
Time limit for renewal of trust services approaching expiration date	All completed requests, related to trust services, automatically generate renewal requests 45 days prior to their expiration date. If the subscriber does not complete the renewal process, the initial deadlines for new applications - payment, identity validation and certificate generation - will be considered.

4 Use restrictions

Qualified certificates for electronic seals issued by GTS are used by 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.

The data and documentation submitted by subscribers relating to entities outside Portuguese territory shall be those issued by the Official Registry of the respective country, duly apostilled and officially translated into Portuguese or English.

The subscriber will only be able to validate the identity: in person (at the headquarters of the company on the island of Madeira or at the offices of the company in: Lisbon, Porto and Ponta Delgada) by videoconference (using electronic identification means, through software certified for this purpose), in Portuguese or English, through payment and scheduling.

Subscribers in possession of a Portuguese identification card can validate their identity using the authentication certificate of the national identity card and/or *chave móvel digital*, through the autenticacao.gov.pt portal (available only to Portuguese citizens, with compatible digital documents/certificates).

Subscribers can validate their identity between 9:00 am and 5:30 pm (mainland Portugal local time).

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. To use the certificate only in the capacity or in accordance with the powers of attorney for which it 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. Validation will be carried out in the framework of 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, in Portuguese or English, (at the headquarters of the company on the island of Madeira or at the offices of the company in: Lisbon, Porto and Ponta Delgada), by prior appointment, accompanied by the original identification document, being present at this act two registry administrators (paragraph a, of No. 1, of article 24 of Reg. 910/2014);
- By videoconference, in Portuguese or English, (through software certified for this purpose), by appointment, ensuring the physical presence of the natural person or an authorized representative of the legal person, with the presence of the original identification document,

complying with the requirements established in Article 8 of Regulation 910/2014 regarding 'substantial' or 'high' security levels and in Decision No. 154/2017 of the National Security Office (*Gabinete Nacional de Segurança* - GNS), (paragraph b, of No. 1, Article 24 of Regulation 910/2014);

- Using the authentication certificate of the Portuguese national identity card and/or *chave móvel digital*, through the autenticacao.gov.pt portal (available only for Portuguese citizens, with compatible digital documents/certificates); 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.

The validations described above will only take place after:

a) The respective payment is done;
b) The submission of requested documents;
c) The confirmation and validation of all data by the registry administrators.

I. In the case of validations by videoconference, you must ensure that you meet the following technical requirements and have the necessary documentation with you:

a) Verify your antivirus restrictions (since some antiviruses do not allow to carry out a videoconference);
b) Use recommended browsers for the videoconference (Google Chrome or Firefox);
c) 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;
d) The videoconference must be held in a well-lit place to allow the verification of the identity card (e.g., the hologram on the national identity card);
e) It is required to use a webcam and a microphone of acceptable quality level;
f) The videoconference can be done through a mobile phone with camera and microphone.
g) Check that you have your identification document (e.g., ID card) and the mobile phone whose number you used to purchase the qualified signature with you;
h) If the technical requirements are not met and a second videoconference is necessary, the customer will be charged a fee of 10.00 euros.

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[1].

[1] Lisbon, Porto, Ribeira Brava (Madeira) and Ponta Delgada (The Azores)

II. 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.

III. 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. DCs Renewal

If the holder wants to renew his/her certificate, and if the functions for which that certificate was issued are maintained, he/she may:

- use the application automatically created by the platform (45 days before the expiration date of the certificate), select the desired payment method and follow the instructions sent by GTS, or
- request the renewal of the certificate with the same data and make the renewal payment, following the instructions sent by GTS.

6.3. DCs Revocation

When a revocation request is verified, it shall be executed within a maximum of 24 hours after receipt of the signed form.

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.

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.
In cases where the holders do not meet the conditions for the completion of the process, GTS will proceed to analyze the process.

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 S*ubject* 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 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;
- The iGEST platform for invoicing;
- The Identity Trust Management AG and Electronic IDentification platforms, as regards videoconferencing for the validation of the identity of qualified electronic signature service holders, who are duly certified to operate with eIDAS Trust Service Providers;
- the CRM - Salesforce, to manage support requests received by e-mail or telephone, as well as to manage sales leads.

12 Preservation of audit logs

Audit logs are preserved for the periods required by legislation (7 years).

13 Availability of services

CRLs can be checked at 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.

Global Trusted Sign has online certificate status OCSP validation services available at: http://ocsp.globaltrustedsign.com.

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

GTS will assume responsibility related to compensations, in accordance with the applicable legislation, in the terms set forth in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014, and the General Data Protection Regulation 2016/679 of 27 April 2016.

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 authorization 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.

Name	**GTS Management Group**
Address	ACIN-iCloud Solutions, Lda Global Trusted Sign Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira - Portugal
E-mail	info@globaltrustedsign.com
Website	https://www.globaltrustedsign.com
Telephone	National: 707 451 451 [1] International: + 351 291 957 888 [2] (Portuguese - Option 1 / English - Option 2; GTS - Option 6) [1]Maximum amount to be paid per minute: 0.09€ (+VAT) for calls from fixed networks and 0.13€ (+VAT) for calls from mobile networks. [2] Cost of an international call to a fixed network, according to the current rate.

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). These officers can be contacted by e-mail dpo@acin.pt or telephone 707 451 451[2] (for international calls, must used + 351 291 957 888[3]).

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:

a) Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
b) Other national and European legislation related to activities of provision of qualified trust services;
c) General Data Protection Regulation 2016/679 of 27 April 2016.

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.

[2] Maximum amount to be paid per minute: 0.09€ (+VAT) for calls from fixed networks and 0.13€ (+VAT) for calls from mobile networks.
[3] Cost of an international call to a fixed network, according to the current rate.

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

_____/____ , _____ , _____.

(place) (day) (month) (year)

_____

(Signature)