TERMS AND CONDITIONS FOR GTS CERTIFICATES

Global Trusted Sign

Document Reference | FO23_GTS_V11

Table of Contents

1 TERMS AND CONDITIONS FOR THE USE OF QUALIFIED AND/OR ADVANCED-CERTIFICATES ISSUED BY GTS

Global Trusted Sign (hereinafter referred to as GTS), as a qualified trust service provider, offers online services that enable the purchase of digital products.

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

2 QUALIFIED AND/OR ADVANCED TRUST SERVICES

These terms and conditions apply to the use of certificates issued by GTS

By using these services, the holder understands that advanced digital certificates have a high trust level, although they cannot guarantee the same probative value than that of qualified certificates.

The holder must read each document before proceeding to purchase the certificate provided by the GTS services.

Regarding SSL certificates, these are used by different holders, systems, applications, mechanisms and protocols with the aim to establish web-based data transmission through SSL/TSL protocols, and in accordance with European Regulation 910/2014, in order to:

- Identify the legal person managing a website: it provides to an internet browser user reasonable assurance that the website to be accessed is managed by a legal person identified in the certificate by its name, registered office, registration in the Institute of Registration and Notary Affairs *(Instituto de Registos e Notariado*), or any other explanatory information.
- Allow encrypted communications with a website: it eases the exchange of encryption keys to allow the transmission of encrypted information through the internet, between an internet browser use and a website.

By providing a more reliable identity verification process, as well as information about the company registered office, Extended Validation (EV) certificates can help to:

- Impede phishing attacks and other identity fraud in certificates;
- Support companies that may have been the target of a phishing attack or identity fraud by providing to users a tool for its identification;
- Support security forces in their investigations on phishing and other identity fraud attacks, supporting, where applicable, the contact, investigation and legal actions against the Holder.

Relying Parties can verify the chain of trust of a certificate issued by GTS, thus ensuring the authenticity and identity of the holder.

SSL certificates allow to protect the security and confidentiality of data provided by the user (Article 32, paragraph 1, letter b) of the GDPR).

The decision of the user to read and sign a document does not affect legal effects derived from that activity.

Regarding the qualified digital signature, the holder understands that the same is equivalent to a handwritten signature, with a probative value in European Union countries, as well as in those countries that have declared the acceptance of Regulation (EU) No.910/2014.

The holder declares that he/she will notify GTS, as well as all relying parties, if his/her electronic mail changes, to ensure the conditions required for the use of these services. Furthermore, the holder declares that, in the case of professional certificates, he/she will notify GTS without delay if he/she no longer meets the professional attributes set forth in the acquired certificate.

The user declares that, when using these services, understands that the certificates are legally binding in Europe and other countries. The holder also declares that he/she understand that printed copies of documents with qualified signatures do not have the same legal value as the originals digitally stored.

3 DATA PROTECTION AND STORAGE

Qualified certificates for electronic signatures can be of two types: single (for a natural person or pseudonym) or collective (for a legal person).

Advanced certificates can be of four types: for natural persons (natural person or pseudonym); for legal persons; for natural persons–professional; and for legal persons-professional.

SSL certificates can be of two types: single (natural person) or collective (legal person).

To obtain the certificate, users must fill in the corresponding form for certificate issuance, in which personal data is requested which, for this reason, is considered to be sensitive.

Within the scope of the GDPR in force, the data stored on the *remote server* for this purpose must follow a set of protection requirements to safeguard the privacy and security of the data of its holders/users.

In this regard, GTS declares that all the data requested and collected arises from the need to guarantee the security means of identification via electronic means, safeguarding the misuse of identity.

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 customer 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	Information of the legal or natural person, required to acquire a service, will be stored during 180 consecutive days. In case of no payment, all the 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	In the case of Qualified Certificates for Electronic Signature (for legal or natural persons) and Qualified Certificates for Electronic Seals, once the payment has been made, the form has been sent and the terms and conditions have been duly signed, the holder will receive a notification to schedule the validation of his/her identity by videoconference (Order 154/2017 of the National Security Office - *Gabinete Nacional de Segurança* - GNS), in person or by authenticating the *cartão de cidadão* (Portuguese national id card). 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 be notified of the need to reschedule within the following 7 days. If the holder's data is not validated within these time limits, all the information will be deleted.
From the identity validation to the issuance of the certificate	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	In the case of qualified certificates for electronic signatures, qualified certificates for electronic seals and certificates for website authentication, if an

Time limits for the storage of information	
	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. For advanced electronic signature and advanced electronic seal certificates, if GTS notices that an account has been inactive for a period of 9 months, the legal person/ natural person/user will be notified that he/she has 180 working days to log in, otherwise the account will be deleted.
Time limit for the right to data portability	When the natural person/legal person/subscriber/user exercises the right to portability, GTS will execute the request within a maximum period of 60 days.
Time limit for exercising the right to be forgotten	In order to comply with legal requirements, some of the information may not be completely deleted, as the legal validity of certificates for a period of 7 years, as set out in recital No 61 of Regulation (EU) 910/2014. Therefore, when holders request 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, from the date of issuance of the certificate. 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

The certificates issued by GTS are used by different holders, systems, applications, mechanisms and protocols with the aim to allow the probative signature of documents, emails, transactions by natural or legal persons, encryption and access control, unequivocally ensuring the identity of the holder, 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 Policy (available at https://pki.globaltrustedsign.com/index.html) and with all the applicable legislation.

The subscriber undertakes not to use the service for any unlawful purpose, not to cause the disruption of the service, not to distribute contents that may breach third parties' privacy, intellectual property rights or other related property rights, or for any other purpose that GTS may

consider 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/Madeira local time).

With regard to SSL certificates, they are focused on the identity of the certificate holder and not in his/her behaviour.

Thus, a certificate for website authentication cannot guarantee that:

- The holder identified in the certificate is effectively providing services;
- The holder identified in the certificate is in conformity with the applicable legislation;
- The holder identified in the certificate is reliable, honest or ethical in conducting his/her operations;
- It is “safe” to establish a commercial relationship with the holder identified in the certificate.

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 if 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 is the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados* - CNPD)- (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 his/her 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 Policy of Advanced Certificates (available at https://pki.globaltrustedsign.com/index.html) as well as with all the applicable legislation;
3. Not to monitor, manipulate or 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 accurate and complete related to any personal and professional data of the holder that GTS may request for the registration process. Any modification of that data must be informed to the 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 case of having knowledge of any unlawful behaviour or access violation involving the qualified certificate, he/she shall notify GTS within a maximum period of 24 hours;
7. For activities done by his/her representatives or agents while using the qualified certificate;
8. To use the certificate exclusively in the capacity or in accordance with the power of attorney for which it was issued;
9. To communicate to GTS the information regarding expired/modified data and make the updated information available. Whenever the certificate holder intends to renew his/her certificate, he/she must confirm the update status of his/her data;
10. To comply with security procedures, as well as all the technical requirements that have been established by GTS;

11. To 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 CERTIFICATE ISSUANCE PROCESS AND HOLDER IDENTITY VALIDATION

Before the issuance of the 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*".

GTS has mechanisms to validate the veracity of all documentation submitted during the fulfilment of the form to buy a product, as well as to "*accredit and verify the identity of natural or legal persons requiring the presentation of electronic means of identification*".

It should be noted that, in case of doubts about the documents submitted, GTS reserves the right to request validation of identity in person or by videoconference (the latter at a cost of 10.00 euros + VAT) with the holder.

The verification of the identity of the subscribers and/or holders will be carried out by the registry administrators working group, before the issuance of the qualified certificate, 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); or;
- By videoconference, in Portuguese or English, (through software certified for this purpose), by appointment, ensuring the physical presence of the natural person or an authorised 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), or

- 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 qualified electronic signature certificate issued in accordance with the previous paragraph (paragraphs c and d, of No. 1, of Article 24 of Reg. 910/2014), applicable to renewals.

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

In order to validate the identity accordingly, it must be taken into account the following:

I. The videoconference / in-person validation (at the headquarters of the company on the island of Madeira or at the offices of the company in: Lisbon, Porto and Ponta Delgada) is only required when the Registry Administrator has any doubt about the authenticity and adequacy of submitted documents.

II. 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, as you will receive an activation code on your mobile phone during identity validation.;

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 with you (e.g., national identity card - hologram); and the mobile phone number you used to buy the certificates;

h) If the technical requirements are not met and a second videoconference is required, the customer will be charged an additional 10.00 euros;

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

The videoconference is recorded for reasons of data 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 locations that GTS facilitates for that effect[1].

I. 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.

II. 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 request created automatically by the platform (45 days before the expiry 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.

6.4 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.

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

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 60 days after the communication to the other party.

7 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 analyse the process.

8 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 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.

9 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 holder must download his/her certificate in his/her personal area in the GTS portal, once the authentication in the portal has been done. To use the certificate, a PIN will be sent, via SMS, to the mobile phone number provided by the user when buying the product. This certificate can be downloaded as many times as necessary

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.

The issuance and use of the certificate are always the responsibility of its holder.

10 SHARING INFORMATION WITH THIRD PARTIES

GTS has the right to share information with the competent authorities, provided that:

- 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, with the data shared being only that necessary to carry out this process;
- 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, when deemed necessary;
- the CRM - Salesforce, to manage support requests received by e-mail or telephone, as well as to manage sales leads.

11 PRESERVATION OF AUDIT LOGS

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

12 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.

13 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.

14 CONTACTS

All stakeholders must use appropriate collective communications means. These means can include 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
Managers	Tolentino de Deus Faria Pereira José Luís de Sousa
Address	ACIN iCloud Solutions, Lda. Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira – Portugal
General e-mail	info@globaltrustedsign.com
Report e-mail	report@globaltrustedsign.com
Website	https://www.globaltrustedsign.com
Phone Number	National: 707 451 451[1] International: + 351 291 957 888[2] (GTS - Option 3) [1] Maximum price per minute: 0.09€ (+VAT) for calls originating on fixed networks and 0.13€ (+VAT) for calls originating on mobile networks; [2] Cost of an international call to a fixed network, according to the tariff in force.

15 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. These officers are available to provide support GTS customers and to cooperate with the appointed national control 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] (or + 351 291 957 888, if calling from abroad[3]).

16 DISPUTE SETTLEMENT PROVISIONS

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

[2] Maximum price per minute: 0.09€ (+VAT) for calls originating on fixed networks and 0.13€ (+VAT) for calls originating on mobile networks.
[3]Cost of an international call to a fixed network, according to the tariff in force.

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

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

17 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, and its conclusions will be transmitted to the supervisory 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:

_____ / _____ _____ , _____

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

_____

(Signature)