TERMS AND CONDITIONS FOR CERTIFICATES FOR WEBSITE AUTHENTICATION

Global Trusted Sign

Document Reference | FO09_GTS_V5

1. Terms and Conditions for the Use of Qualified 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 with the certificate subscriber and holder.

2. Qualified Trust Services

These terms and conditions apply to the use of SSL certificates issued by GTS.
SSL certificates 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 the GTS TSA, thus ensuring the authenticity and identity of the holder.
SSL certificates allow to protect the security and confidentiality of data provided by the user (Art. 76 - GDPR).

3. Data Protection and Storage

SSL Certificates can be of two types: single or collective. In both cases, users must fill in a website certificate 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 their holders.

In this regard, GTS declares that all data requested and collected is derived from the need to guarantee security means of identification by electronic means, to avoid any 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 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	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.
Period of inactivity	If GTS identifies an account that has been inactive for 9 months, it will notify to 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	When the 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 signatures must be guaranteed for extended periods, defined by the Certification Authority (CA) as 7 years. 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.

4. Use restrictions

SSL certificates 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.

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 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 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 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 GTS Certification Practice Statement and Certification Policies (available at https://pki.globaltrustedsign.com) and with all the applicable legislation;
3. Not to monitor, manipulate or perform "reverse engineering" activities on the technical implementation (hardware and software) of 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 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. Communicate to GTS information regarding expired/changed data and make available the updated one. Whenever the holder intends to renew his/her certificate, he/she must confirm the updated status of his/her data;

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. Holder identity validation

Prior to the issuance of a qualified type certificate, GTS is committed to ensure that the identity of the holder is in fact the person to whom that identity has been assigned. For this purpose, GTS has mechanisms to validate the veracity of all documentation submitted during the fulfilment of the form to buy a product. 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, in order to "accredit and verify the identity of natural or legal persons requiring the presentation of electronic means of identification".

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).

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 the case of validations by videoconference, it must be taken into account the following:

I. The videoconference validation is only required when the Registry Administrator has any doubt about the authenticity and adequacy of submitted documents.

II. In case of validation by videoconference it must, previously, be taken into account that you meet the following technical and documentation requirements:

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 certificate 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 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 places that GTS facilitates for that effect[1].

7. GTS obligations

The Certification Authority (CA), as the entity responsible for processing the holder data, is committed to ensure through its mechanisms, principles of fairness, loyalty, transparency, minimization, storage 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.

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

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 subscribed 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 paid.
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 use of the certificate is always responsibility of its holder.

The use of the certificate is only permitted, and where applicable depending on 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 and in the properties of the certificate as required by the applicable legislation.

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;
- 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.

11. Preservation of audit logs and other documents

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 scheduled maintenance downtime, 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 within 24 hours. During that time, 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 GTS Certification Authority.

GTS 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 quality control purposes, with the due authorisation of the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados* - CNPD). If you do not want your call to be recorded, we recommend that you contact us by alternative means.

Name	**GTS Management Group**
Address	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.

15. Contact of the Data Protection Officer

In case of any doubt or any event related to data protection, GTS users can contact the Data Protection Officer (DPO – Art. 37, GDPR), appointed by 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[2] (for international calls, must used + 351 291 957 888[3]).

16. 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 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 eventually 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.

[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)