TERMS AND CONDITIONS OF THE VIDEOIDENTIFICATION

PROCESS AND ISSUANCE OF LONG-TERM CERTIFICATES

QES MULTI

On the one Hand, SIGNICAT, S.L.U ("formerly known as Electronic Identification S.L."), whose registered address is located at Avenida Ciudad de Barcelona 81, 4ª Planta, registered in the Business Register of Madrid on March 13th, 2013, with ID number B-86681533, (hereinafter referred to as "SIGNICAT SLU"), is a Qualified Provider of Trust Services, which acts in accordance with the provisions of Regulation (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL dated July 23rd, 2014 regarding Electronic Identification and Trust Services for Transactions Electronic Systems within the Internal Market, thus repealing Directive 1999/93 / EC, as well as the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly EN 319 411-1 and EN 319 411-2, in order to facilitate compliance with legal requirements and international recognition of its services.

And on the other Hand, **The APPLICANT/SUBSCRIBER**, whose identification data for the purposes of this contract are stated in his/her Identification Document in use and in the video generated as a result of the Video Identification and Issuance of the Certificate process.

1. OBJECTIVE

The purpose of this document is to inform the Applicant/Subscriber in a clear and understandable manner of the present *"Terms and Conditions of the remote identification process by unassisted video and the Conditions of the Electronic Certification Service for the issuance of long-term certificates duration"* and regulate the services in accordance with the terms provided in this document, the Certification Practices Statement, the eIDAS Regulation and local Laws which may be applicable.

Said prior identification process is necessary to prove the identity of the Applicant/Subscriber, who requests SIGNICAT SLU to issue a qualified long-term electronic signature certificate of natural person ("Certification Services"), a certificate whose use is subject to the conditions of the Electronic Certification service provided by SIGNICAT SLU as a Qualified Provider of Trust Services described below.

2. APPLICABLE DEFINITIONS

- **CERTIFICATION AUTHORITY (CA)**: trusted entity of the sender and the receiver of the message. This trust of both in a 'trusted third party' allows either to trust in turn the documents signed by the Certification Authority, in particular the documents which identify each public key with its corresponding owner and are called certificates. In providing the Service requested by the Applicant/Subscriber, SIGNICAT SLU will act as the Certification Authority relating a given public key linked to a given Applicant/Subscriber through the issue of a certificate**.**

- **REGISTRATION AUTHORITY (RA)**: entity which, among other functions, uniquely identifies the Applicant/Subscriber for a certificate and, where applicable, the other circumstances associated with the Certificate in accordance with the provisions of Section 1.3.2. Registration Authorities of SIGNICAT SLU's CPS. The Registration Authority provides the Certification Authority with the verified details of the Applicant/Subscriber in order for the Certification Authority to issue the corresponding certificate. Any or all of the RA's own functions may be assumed either directly by SIGNICAT SLU or by any entity authorized by SIGNICAT SLU.

- **ELECTRONIC SIGNATURE CERTIFICATE**: electronic statement which links the validation data of a signature to a natural person and confirms, at least, the name or pseudonym of that person.

- **QUALIFIED ELECTRONIC SIGNATURE CERTIFICATE**: electronic signature certificate which has been issued by a Qualified Provider of Trust Services and meets the requirements set out in Annex I of EU Regulation 910/2014 of July 23rd, 2014 (eIDAS Regulation), offering the highest legal guarantees in terms of identification of the signatory and his/her linking to the signature in a unique way, integrity and non-repudiation of the data as they are linked to the signature.

- **CERTIFICATION PRACTICES STATEMENT ("CPS")**: document drawn up by a Certification Authority which includes or regulates the provision of Certification Services by said Certification Authority in its capacity as Certification Service Provider, in this case, SIGNICAT SLU. It regulates, among other things, the management of the Signature creation and verification Data and of the Certificates, the conditions applicable to the request, issue, use, suspension and termination of the validity of the Certificates.

- **QUALIFIED ELECTRONIC SIGNATURE**: advanced electronic signature which is created by means of a qualified electronic signature creation device and is based on a qualified electronic signature certificate. The validity of the signature is iuris tantum because it is a qualified signature, the burden of proof rests on the person who rejects the signature as valid.

- **QUALIFIED TRUST SERVICE PROVIDER**: trust service provider that provides one or more qualified trust services and has been granted qualification by the supervisory body.

- **APPLICANT/SUBSCRIBER or APPLICANT/SUBSCRIBER**, which is the natural person identified in the header who contracts the SIGNICAT SLU certification services and who, prior to the issuance of the qualified certificate, applied for and successfully completed the SIGNICAT SLU Video Identification Process.

3. TERMS AND CONDITIONS OF THE VIDEO IDENTIFICATION PROCESS

The Identification Process of the Applicant/Subscriber for the Identification Services provided by SIGNICAT SLU in order to issue electronic certificates shall be carried out by one of the following means, in accordance with Article 24.1 eIDAS:

a) in the presence of the natural person or an authorized representative of the legal entity, for which the Applicant/Subscriber must go to SIGNICAT SLU offices at Av. de la Ciudad de Barcelona, 81, 4, 28007 Madrid, given that there are no delegated Registration Authorities.

b) remotely, using electronic identification means, for which the presence of the natural person or an authorized representative of the legal person has been authorized prior to the issuance of the qualified certificate, and in accordance with the video-identification process referred to in this document and the Certification Practice Statement, accessible through the following link https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

c) by means of a qualified electronic signature certificate or a qualified electronic seal issued in accordance with point (a) or (b)

d) using other nationally recognized methods of identification which provide security equivalent in terms of reliability to physical presence. Equivalent security shall be confirmed by a conformity assessment body.

3.1 IDENTITY VALIDATION BY ELECTRONIC MEANS AND DESCRIPTION OF THE VIDEO-IDENTIFICATION PROCESS

The Video Identification Process (hereinafter referred to as the "Video Identification Process" or the "Process") is a method of real-time and unattended remote video identity verification through an application developed and owned by SIGNICAT SLU (the "Application") which implements, assists and records the entire Process of the person registration and allows to validate identity documents remotely. Such video captures and validates the identity document in real time and in an automated manner (approximately 10-20 seconds) and is carried out by SIGNICAT SLU through its qualified human Agents who, as verification operators acting as Registration Authority, are in charge of accrediting the identity.

3.1.1 General Information on the Video Identification Process

The Applicant/Subscriber accesses the Application and the interface prior to initiating the actions suitable in order to verify the identity and **is requested to read and express his/her acceptance with the present document, as well as freely grant his/her consent for the processing of biometric data necessary to perform the video identification**. To do so, SIGNICAT SLU previously provides the Applicant/Subscriber with the Privacy Policy which contains the processing of personal data which will be carried out during the Process in compliance with the provisions of the Data Protection regulations.

In the event that the Applicant/Subscriber does not give this consent, the Process cannot continue, and the Applicant/Subscriber must resort to one of the alternatives for identification determined in Clause One of this document in accordance with the provisions of Article 24.1 of the eIDAS Regulation.

Finally, and prior to the start of the Video Identification Process, the user will be asked for a telephone number in order to send an OTP in order to link the identity of the Applicant/Subscriber with the device and the telephone number he/she uses to carry out the Process.

Once the Applicant/Subscriber has read, accepted and expressed his/her agreement with the Process, they will proceed to carry out the necessary Video Identification in order for SIGNICAT SLU to proceed with the issuance of the qualified natural person certificate.

The Applicant/Subscriber is guided at all times by voice and text during the Video Identification Process and, by means of the Application, an automated control of the elements of the environment (lighting conditions, network, quality of the camera) is carried out in order to obtain an optimal recording of the Video Identification and its evidence.

In this sense, the steps of the Process prior to the issuance of the qualified certificate are as follows:

The first step of the Process indicates to the Applicant/Subscriber that he/she has to show the identity document to be used in order to perform an Image comparison with the original documents through a specialized technology to verify the authenticity of the document and to perform the data extraction

(OCR) of the MRZ or other parts of the document, and the possibility to call the credentials in real time.

Therefore, the front side of the ID document used by the Applicant/Subscriber during the Process will be captured. To do so, the Applicant/Subscriber will be asked to show the front of his/her document and fit the image in the box shown.

When the capture is completed, a confirmation message is displayed, and the next part of the Process continues.

The next step consists of capturing the back of the document. The Applicant/Subscriber will be asked to show the back of his/her document and fit the image in the box shown.

When the capture is complete, a confirmation message is displayed, and the next part of the Process continues.

The biometric data of the Applicant/Subscriber is then captured in order to perform a real-time comparison with the image of the identity document for a facial recognition process based on automatic biometric scoring. For this purpose, the Applicant/Subscriber is asked to show his/her face and to fit the image into the box displayed on the screen.

When the biometric data has been captured, the Applicant/Subscriber is asked as proof of life to execute a facial movement to the camera and, if everything is correct, a message of conformity is displayed, and the next part of the Process continues.

Whenever the entire Process is successful, the Applicant/Subscriber is informed that the Video Identification Process has been completed and that the evidence generated during the Process will be checked and validated by means of the Registration Authority Verification Tool for review of the Process by a qualified human being previously trained by specific training.

At this point, the Application places the Video Identification and the data generated during the same at the disposal of a qualified human Agent in charge of verifying the identity of the Process Applicant/Subscriber and requests the asynchronous review of the recorded video, as well as the rest of the evidence and elements obtained during the Process. The average verification time for an agent is approximately three minutes.

3.1.2. Security Elements of the Video Identification Process and Validation by a Qualified Human Agent

For the asynchronous review by a Qualified Human Agent, there is a security protocol based on EU good practices that is supported by the tool offered to the Qualified Human Agent in which the evidence obtained during the Process are shown, as well as the flags or notifications of those not obtained.

The recording of the video, the request for verification of the Video Identification as well as the ruling of the Qualified Agent are traced within the Application, and a time stamp is applied to each trace in order to guarantee its coherence and integrity.

Therefore, the Process ensures the chain of custody of the verification from the evidence collected by the Process to the traces linking the identification to the Qualified Human Agent of the Registration Authority. Thus, the result is a verified identity with technical security equivalence to that performed in the physical presence of the Applicant/Subscriber.

Once the identity is positively validated by the Qualified Human Agent, the identity of the Applicant/Subscriber is accredited, and he/she will be enabled to continue and receive the SIGNICAT SLU Electronic Certification Service which allows him/her to continue with the qualified certificate issuance process of natural person and the signature of electronic documents.

Shall the result of the Process be negative, the Process for issuing qualified certificates cannot continue, and the Applicant/Subscriber must physically go to the SIGNICAT SLU premises to carry out an in-person verification of their identity.

3.2 APPLICANT/SUBSCRIBER OBLIGATIONS IN RELATION TO THE VIDEO IDENTIFICATION PROCESS.

The Applicant/Subscriber, throughout the whole Process, undertakes to:

- Use the Service in accordance with the provisions of this document, the CPS, the particular conditions which may be applicable, and with any other instruction, manual or procedure provided by SIGNICAT SLU.

- That the document used during the Process is an authentic, legally valid document and that, in addition:

    - It is not a photocopy or printed card.
    - It is not in digital format (mobile, tablet or computer).
    - It is not in a cover.
    - It is not damaged and is complete, with all the security elements being contained within the document.

- That during the Process and the recording of the video, in order to avoid rejection:

    - The lighting conditions in the video must allow the face of the identified person and the document to be clearly seen.
    - The stream of the video must be constant, without cuts or delays.
    - A living person must show the identification.
    - If another person, other than the person to be identified, is carrying out the entire Process, the identification will be rejected as ungenuine.
    - If someone else is present in the video but is clearly not coercing the person to be identified, the identification may be valid, as in the case where a particular person is helping a disabled person to make the identification.
    - It must be possible to clearly visualize all parts of the captures of the document, obverse, reverse and face of the person.

- The Applicant/Subscriber cannot be asleep or show signs which may be interpreted as being under the influence of drugs or alcohol.

3.3 ISSUANCE, DELIVERY AND ACCEPTANCE OF THE CERTIFICATE

3.3.1 Certificate Request and Keys Generation by SIGNICAT SLU on behalf of the Applicant/Subscriber.

Once the Video Identification Process is completed, the Applicant/Subscriber will request and authorize SIGNICAT SLU on his/her behalf to eventually generate and manage the keys, private and public, which allows SIGNICAT SLU to proceed with the issuance of the qualified long-term certificate for natural person and sign on his/her behalf the appropriate electronic documents with third parties of a public or private nature whom SIGNICAT SLU maintains certain contractual agreements with, therefore in accordance with the provisions of Clauses 3.3.3, 3.3.4 and 3.3.5.

3.3.2 Information veracity

The APPLICANT/SUBSCRIBER shall be responsible for ensuring that all information provided to SIGNICAT SLU either directly or through the identity document used during the certificate issuance process is accurate, complete for the purpose of the certificate, and that it is up to date at all times, for which he/she guarantees to use a legal and valid identity document, without it having been altered and/or modified by the APPLICANT/SUBSCRIBER or third parties.

3.3.3 Authentication PIN setting and Issuance of the Certificate

For the issuance of the certificate, SIGNICAT SLU will use the data of the identity document provided by the Applicant/Subscriber during the Video Identification Process. Said data will be extracted by SIGNICAT SLU and incorporated into the electronic certificate for the purpose of linking his/her identity to it, once confirmed by the Applicant/Subscriber.

Once the video identification process is completed, the Applicant/Subscriber will receive or have the option to choose an authentication PIN code that will allow him/her to be associated as a user to his/her electronic certificate.

3.3.4 Acceptance of the Certificate Issuance and Ratification of the present Terms and Conditions.

Once the Applicant/Subscriber has received or chosen the authentication PIN code, he/she must confirm that it is in his/her possession for the purpose of accepting the issuance of the electronic certificate, and these Terms and Conditions which shall be previously shown to you and will be sent to you subsequently by email, already electronically signed by the Applicant/Subscriber.

3.3.5 Delivery of the Certificate

Within the process of issuing, there is no specific delivery of the certificate to the Applicant/Subscriber. SIGNICAT SLU will manage it in its capacity as Qualified Trust Service Provider, in order for the Applicant/Subscriber to use it for the electronic signature of documents.

3.4 SERVER SIGNATURE SERVICE

Once the identification process is completed, the identity is validated by the verifying agent, the identity of the Signatory shall be guaranteed and SIGNICAT SLU, as a Qualified Trust Service Provider, will safely store the user's electronic certificate in order for the latter to use it during its term to sign documents electronically.

The use of this PIN to sign documents entails the statement of the consent of the Applicant/Subscriber to be linked to their content.

Each time the user wishes to sign a document electronically using the generated electronic certificate, he/she must access the specific area where the user can view its content.

In case of being satisfied with its content and wishing to be linked by means of its electronic signature, the user must continue with the process.

At that time, the platform will request his/her PIN code and once the PIN has been entered, he/she will receive an OTP on his/her cell phone which will be included in the specific section within the signature environment. The introduction of this OTP will enable SIGNICAT SLU to apply the signature creation data of the Applicant/Subscriber in order to generate the electronic signature of the previously displayed document.

The PIN code in conjunction with the OTP input, guarantees the exclusive control of the electronic certificate for signing the documents.

SIGNICAT SLU grants the Applicant/Subscriber, on a non-exclusive and non-transferable basis, a license to use the copies of SIGNICAT SLU cryptographic secure device software for the operation of the signature device when applicable, as well as for the production of the electronic signature, certificate and the remaining cryptographic services by the signatories.

In the event that any person other than SIGNICAT SLU makes modifications to the supplied software, all warranties in respect of the software shall be immediately cancelled.

4. GENERAL CONDITIONS OF THE TRUST SERVICE

4.1 GENERAL CONDITIONS OF THE VIDEO IDENTIFICATION SERVICE

- **Information conservation period**

All information related to the Process of issuing qualified electronic certificates for natural persons, including the biometric information, will be kept by SIGNICAT SLU during the validity period of the contractual relationship, as long as the deletion of the same is not requested and during the limitation period of the legal actions that could be raised, or claims that could be received on behalf of official bodies.

In this sense, the maximum period of conservation of the relevant information in relation to the Process of Video Identification and issuance of qualified certificates, that is, a copy of the video

recording, the photos or screenshots of the Applicant/Subscriber and the identity document used, the automatic result of the verification carried out by the SIGNICAT SLU Application, as well as the evaluation and observations made by the qualified human identity verification Agents, along with their decision to approve or reject the identification, shall be 15 years from the moment of issuance of the certificate, unless otherwise stipulated by law. Once the contractual relationship has ended, the Applicant/Subscriber's data will be duly blocked, in accordance with the provisions of the applicable regulations.

In addition, it is advised that all evidences of incomplete identification processes which have not been completed due to suspicion of attempted fraud will be kept for a period of 5 years from the execution of the Process, specifying the reason why they were not completed, in accordance with the policy established for this purpose.

- **Limitation of Liability in relation to the Video Identification Process.**

Process quality: SIGNICAT SLU guarantees the adequate performance of the Video Identification Services described in this document provided that the means made available to the Applicant/Subscriber are used properly and in accordance with SIGNICAT SLU's instructions.

Access to and use of the Video Identification Services do not imply an obligation on the part of SIGNICAT SLU to control the absence of viruses, worms or any other harmful computer element. It is up to the Applicant/Subscriber as a user, to have adequate tools for the detection and disinfection of harmful computer programs at all times. SIGNICAT SLU cannot be held responsible for any damage caused to the Applicant/Subscriber's computer equipment or third parties during the Video Identification Process.

Process availability: The operation of the Video Identification Process may depend on a correct configuration of the equipment from which the user accesses and starts the Video Identification Process, so the user must therefore follow the instructions offered and, in any case, have both software and hardware requirements specified at all times.

Likewise, in order to carry out the Video Identification Process, an Internet access line must be available. The operation of the Video Identification Process may depend on the adequate quality and speed of the connection through which the Applicant/Subscriber accesses the application, for which he/she will be solely responsible for the provision of telecommunications lines, Internet subscriptions or connections or any other technical means necessary in order to access to and use his/her data.

SIGNICAT SLU shall not be held responsible for damages derived from or related to the non-execution or defective execution of the obligations of the Applicant/Subscriber, nor for the incorrect use of the results of the Process and the keys, nor for any indirect damage which may result from the use of the Process or the information provided by SIGNICAT SLU.

SIGNICAT SLU shall not be held responsible for any inaccuracies in the identification of the Applicant/Subscriber which result from the information provided by the latter during the Process.

SIGNICAT SLU shall not be held responsible for the correct operation of applications which are not approved, and for damages generated by the impossibility of using said applications by the Applicant/Subscriber.

4.2 GENERAL CONDITIONS OF ELECTRONIC CERTIFICATION SERVICES OF LONG-TERM CERTIFICATES.

- **Legal Framework for the Provision of the Service**

The SIGNICAT SLU certification services are technically and operationally regulated by the Certification Practices Statement and the SIGNICAT SLU Certification Policies, and by their subsequent updates, as well as by complementary documentation provided to the APPLICANT/SUBSCRIBER.

The present general conditions, the Certification Practices Statement and the Certification Policies, if applicable to the certificate issued, constitute the legal framework which will regulate the relationship between SIGNICAT SLU and the APPLICANT/SUBSCRIBER, both internally and before third parties, without prejudice to the provisions of current legislation.

The present document constitutes the most relevant aspects and requirements of the rights and obligations of the parties.

The applicable Certification Practice Statement (CPS) and Specific Certification Policies (CP) are incorporated into this document by reference. The latest updated version of the CPS will be accessible at all times and free of charge in the following languages through the link provided below:

Spanish: https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firma-electronica

English: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

In the event of discrepancies, the meaning of the terms contained in this document will prevail with respect to what has been set out in the CPS.

- **Duration of the Contract**

The present Agreement shall be valid for the duration of the issue and expiry dates indicated in the Qualified Certificate for Natural Person requested and contracted by the Applicant/Subscriber from SIGNICAT SLU.

- **Correct Use Obligations**

The APPLICANT/SUBSCRIBER must use the certification service provided by SIGNICAT SLU exclusively for the uses authorized in the CPS, which are known and accepted by the APPLICANT/SUBSCRIBER through having read the document and having ticked the selection box options included in the process.

The APPLICANT/SUBSCRIBER undertakes to use the digital certification service and any other technical element delivered by SIGNICAT SLU and the certificates, in accordance with these terms and conditions, the DPC and the PC's which may be applicable, the particular conditions outlined in the manual where applicable, and with any other instruction, or procedure provided by SIGNICAT SLU to the APPLICANT/SUBSCRIBER and in compliance with any legal provisions which may be in force.

The contracting of the Certification Service with SIGNICAT SLU only admits the use of the Certificate within the scope of the APPLICANT/SUBSCRIBER's official activity, in accordance with the purpose of the type of certificate requested, i.e., the qualified certificate of electronic signature of a natural person of long duration. Once the certificate has been issued, the APPLICANT/SUBSCRIBER may not, unless specifically otherwise agreed between the parties, use the certificate for any commercial purposes. Commercial use of the certificate is understood to be any action by means of which the APPLICANT/SUBSCRIBER offers services to third parties outside this contract, whether for a fee, or free of charge, which require the use of the issued certificate.

- **Prohibited Transactions**

The digital certification services provided by SIGNICAT SLU have not been designed or allowed to be used or resold as equipment to control dangerous situations, or for uses that require error-proof actions, such as the operation of nuclear facilities, navigation systems or air communication, air traffic control systems or weapons control systems, where an error could directly cause death, or facilitate physical damage or serious environmental damage.

- **SIGNICAT SLU Obligations and Responsibilities**

a) In relation to the Provision of the Service as Registration Authority.

SIGNICAT SLU undertakes to register the certificate data and its subsequent issuance to the APPLICANT/ SUBSCRIBER, for which it must carry out the checks it deems necessary regarding the identity and other personal and complementary information of the APPLICANT/SUBSCRIBER and, where appropriate, of the Signatories themselves.

These verifications must include the documentary justification provided by the APPLICANT/ SUBSCRIBER, and if SIGNICAT SLU deems it necessary, any other relevant document and information provided by the APPLICANT/SUBSCRIBER.

In the event that SIGNICAT SLU detects errors in the data that must be included in the certificates or that justify this data, it may make the changes it deems necessary before issuing the certificate or suspend the issuance process and manage the corresponding incident with the APPLICANT/SUBSCRIBER.

In the event that SIGNICAT SLU corrects the data without prior management of the corresponding incident with the APPLICANT/SUBSCRIBER, it must notify the ultimately certified data to the APPLICANT/SUBSCRIBER.

SIGNICAT SLU reserves the right not to issue the certificate, when the documentary justification provided is insufficient for the correct identification and authentication of the APPLICANT/SUBSCRIBER or when the Video Identification Process carried out prior to the issuance of the certificate has not been confirmed as valid by SIGNICAT SLU.

The above obligations will be suspended in the event that the APPLICANT/SUBSCRIBER acts as Registration Authority and has the technical elements corresponding to the generation of keys and issuance of certificates at his/her disposal.

b) In relation to the Provision of the Certification Service.

SIGNICAT SLU undertakes to comply with the obligations established in Law 6/2020, dated November 11th, which regulates certain aspects of electronic trust services, and especially to:

a) Issue, deliver, manage, suspend, revoke and renew certificates, in accordance with the instructions provided by the APPLICANT/SUBSCRIBER, in the cases and for the reasons described in SIGNICAT SLU CPS.

b) Execute the services with the appropriate technical and material means, and with personnel who meet the qualification and relevant experience conditions set out in the CPS.

c) Comply with the service quality levels, in accordance with what is established in the CPS, in technical, operational and security aspects.

d) Communicate the status of the certificates in accordance with what is established in the CPS for the different certificate verification services to third parties who request it.

e) *Process Quality*: SIGNICAT SLU guarantees the adequate performance of the Certification Services described in this document provided that the means made available to the APPLICANT/SUBSCRIBER are used properly and in accordance with SIGNICAT SLU's instructions.

Access to and use of the Certification Services do not imply an obligation on the part of SIGNICAT SLU to control the absence of viruses, worms or any other harmful computer element. It is up to the APPLICANT/SUBSCRIBER as a user, to have adequate tools for the detection and disinfection of harmful computer programs at all times. SIGNICAT SLU cannot be held responsible for any damage caused to the APPLICANT/SUBSCRIBER's computer equipment or third parties during the Video Identification Process.

f) Process Availability: The operation of the Certification Process may depend on a correct configuration of the equipment from which the user accesses and starts the video identification process, so the user must therefore follow the instructions offered and, in any case, have both software and hardware requirements specified at all times.

Likewise, in order to carry out the Video Identification Process, an Internet access line must be available. The operation of the Video Identification Process may depend on the adequate quality and speed of the connection through which the APPLICANT/SUBSCRIBER accesses the application, for which he/she will be solely responsible for the provision of telecommunications lines, Internet subscriptions or connections or any other technical means necessary in order to access and use his/her data.

- **As Provider of Certification Services.**

SIGNICAT SLU shall:

a) Publish truthful information in accordance with Law 6/2020, dated November 11th, which regulates certain aspects of electronic trust services and Regulation (EU) 910/2014.

b) Not to stock or copy, by itself or through a third party, the data of creation of signature, except in the case of their management on behalf of the holder for the purpose of applying the private keys for signature creation, as indicated by the APPLICANT/SUBSCRIBER through the OTP system that SIGNICAT SLU makes available to the APPLICANT/SUBSCRIBER for the signing of electronic documents. In this case, they will use reliable systems and products, including secure electronic communication channels, and appropriate technical and organizational procedures and mechanisms will be applied to ensure that the environment is reliable and is used under the exclusive control of the certificate holder. In addition, they must safeguard and protect the signature creation data against any alteration, destruction or unauthorized access, as well as guarantee its continuous availability.

c) Offer a consultation service on the status of validity or revocation of the issued certificates accessible to the public.

d) Comply with the following additional obligations:

1. The period of time during which they must keep the information related to the services provided in accordance with Article 24.2.h) of Regulation (EU) 910/2014, shall be 15 years from the expiration of the certificate or the end of the service borrowed. In the event that qualified certificates of electronic seal or Website authentication are issued to legal persons, the trust service providers will also record the information that allows determining the identity of the natural person to whom the aforementioned certificates have been delivered, for their identification in judicial or administrative proceedings.

2. Establish civil liability insurance to a minimum amount of 1,500,000 euros, unless the provider belongs to the public sector. If you provide more than one qualified service than those provided for in Regulation (EU) 910/2014, an additional 500,000 euros will be added for each additional type of service. The aforementioned guarantee may be totally or partially replaced by a guarantee through a bank guarantee or surety insurance, so that the sum of the amounts insured is consistent with the provisions of the previous paragraph. The amounts and the means of assurance and guarantee established in the two previous paragraphs may be modified by royal decree.

3. In the event of termination of its activity as a Qualified Trust Service Provider, notify the clients to whom it provides the services and the supervisory body at least two months in advance of the effective termination of the activity, by a means that proves effective delivery and receipt whenever feasible. The service provider's termination plan may include the transfer of clients, once the absence of opposition has been proven, to another qualified provider, who may keep any information regarding the services provided until then. Likewise, it will notify the supervisory body of any other relevant circumstance that may prevent the continuation of its activities. In particular, he must inform of the opening of any insolvency process which is followed against him as soon as he becomes aware of it.

4. Send the conformity assessment report to the Ministry of Economic Affairs and Digital Transformation under the terms provided for in Article 20.1 of Regulation (EU) 910/2014. Failure to comply with this obligation will entail the withdrawal of the qualification from the provider and the service that it provides, and its elimination from the trust list provided for in Article 22 of the aforementioned Regulation, after requiring the service provider to cease the aforementioned breach.

e) SIGNICAT SLU will assume all responsibility towards third parties for the actions of the persons or other service providers to whom they delegate the execution of any or all of the functions necessary for the provision of electronic trust services, including the identity verification actions prior to the issuance of a qualified certificate.

- **GUARANTEES FOR CERTIFICATION SERVICES**

SIGNICAT SLU Guarantee for Electronic Certification Services.

SIGNICAT SLU guarantees that the private key of the Certification authority used to issue certificates has not been compromised, unless otherwise communicated through the certification registry, in accordance with the CPS.

SIGNICAT SLU only guarantees the APPLICANT/SUBSCRIBER, at the time of issuance of the certificate, that:

a) Where appropriate, the certificates are qualified under the terms provided in Law 6/2020, dated November 11th, which regulates certain aspects of electronic trust services.

b) SIGNICAT SLU has neither originated nor introduced false or erroneous statements in the information contained in any certificate, nor has it failed to include necessary information provided and verified by the APPLICANT/SUBSCRIBER.

c) All certificates meet the formal and content requirements set forth in SIGNICAT SLU CPS and PC.

d) SIGNICAT SLU has complied with the procedures as described in the CPS.

SIGNICAT SLU applies reasonable diligence to ensure that each product supplied in the provision of its services is free of computer viruses, worms and other illegal codes, and is obliged to notify the APPLICANT/SUBSCRIBER of any virus, worm or other illegal code subsequently discovered in any product.

- **GUARANTEE EXCLUSIONS**

SIGNICAT SLU does not guarantee any software used by the certificate APPLICANT/SUBSCRIBER or the Signatory, or any other person, to generate, verify or otherwise use any digital signature or digital certificate issued by SIGNICAT SLU, except where there is a written statement from SIGNICAT SLU to the contrary.

- **LIMITATIONS OF LIABILITY AS PROVIDER OF ELECTRONIC TRUST SERVICES.**

SIGNICAT SLU, insofar as it is within the limits established by the applicable law, will not be held responsible for any damages and losses caused to the person to whom it has provided its services or to third parties in good faith, if this occurs in any of the cases provided for under Regulation (EU) 910/2014 or in the following:

a) Failure to provide the trust service provider with truthful, complete and accurate information for the provision of the trust service, in particular, on the data which must be included in the electronic certificate or that are necessary for its issuance or for the extinction

or suspension of its validity, whenever its inaccuracy has not been detected, acting with due diligence, by the service provider.

b) The lack of communication without undue delay to SIGNICAT SLU of any modification of the circumstances that affect the provision of the trust service, in particular, those reflected in the electronic certificate.

c) Negligence in the preservation of the signature creation data or Website authentication, in the assurance of its confidentiality, and in the protection of all access or disclosure of these or, where appropriate, of the means which give access to them.

d) Not to request the suspension or revocation of the electronic certificate in case of doubt regarding the maintenance of the confidentiality of the signature creation data, seal or Website authentication or, where appropriate, of the means that give access to them.

e) Not to use the signature creation data, seal or Website authentication when the period of validity of the electronic certificate has expired, or the trust service provider notifies you of the termination or suspension of its validity.

SIGNICAT SLU will also not be held liable for damages if the recipient acts negligently.

It will be understood that the recipient acts negligently when he does not take into account the suspension or loss of validity of the electronic certificate, or when he does not verify the electronic signature or seal.

SIGNICAT SLU will not be held responsible for damages in case of inaccuracy of the data contained in the electronic certificate if these have been accredited by means of a public or official document, or registered in a public registry if it is required to do so.

- **APPLICANT/SUBSCRIBER LIABILITY**

The APPLICANT/SUBSCRIBER must answer before any person for the breach of their obligations and especially in regard to identification activity or, where appropriate, to Registration Authority, according to these Terms and Conditions.

The APPPLICANT/SUBSCRIBER is responsible for all electronic communications authenticated by means of a digital signature generated with his private key, whenever the certificate has been validly verified through the mechanisms and conditions set out by SIGNICAT SLU.

As long as the notification established in this document does not take place, any responsibility which may arise from the unauthorized and / or improper use of the certificates remains the duty of the APPLICANT/SUBSCRIBER.

- **SUITABILITY OF PRODUCTS WHICH MAKE USE OF IDENTIFICATION, ELECTRONIC SIGNATURE OR ENCRYPTION**

SIGNICAT SLU will not be held responsible for the adequacy of the products and services related to digital certification, identification, electronic signature or encryption existing in the market and which are used in APPLICANT/SUBSCRIBER's computer applications, except when SIGNICAT SLU provides them. In this case, the parties will be subject to the corresponding conditions of use.

- **OWNERSHIP OF CERTIFICATES**

The supplied certificates remain the property of the APPLICANT/SUBSCRIBER.

- **TERMINATION**

The termination will take place in the following cases:

a) Due to a breach by the other party of any of its obligations, if this infraction has not been resolved.

b) Within thirty days from the receipt of the notification made by the party which has not failed to fulfill its obligations.

c) Immediately, if the breach compromises the security of the services.

d) Due to the concurrence of any other cause for early resolution established by current legislation and, especially, by current legislation on electronic signature digital certification.

- **CONFIDENTIALITY POLICY**

SIGNICAT SLU cannot disclose and cannot be compelled to disclose any confidential information regarding certificates without a specific prior request from:

a) The person with respect to whom SIGNICAT SLU has the duty to keep the information confidential, or

b) A judicial, administrative or any other prospective order under the legislation in force.

However, the APPLICANT/SUBSCRIBER accepts that certain information, both personal and otherwise, provided in the certificate request, be included in their certificates and in the certificate status verification mechanism, and that the aforementioned information is not deemed confidential by legal imperative.

- **REIMBURSEMENT POLICY**

SIGNICAT SLU will not reimburse the cost of the certification service in any case.

- **INFORMATION CONSERVATION PERIOD**

All information related to the Process of issuing qualified electronic certificates for natural persons, including the contract duly formalized by the APPLICANT/SUBSCRIBER, the logs generated throughout the issuance event, will be kept by SIGNICAT SLU during the validity period of the contractual relationship, as long as the deletion of the same is not requested and during the limitation period of the legal actions that could be raised, or claims that could be received on behalf of official bodies.

In this sense, the maximum period of conservation of the relevant information in relation to the Process of qualified certificates issuance shall be 15 years from the moment of issuance of the certificate, unless otherwise stipulated by law. Once the contractual relationship has ended, the APPLICANT/SUBSCRIBER's data will be duly blocked, in accordance with the provisions of the applicable regulations.

5. COMMON PROVISIONS

5.1. PLACE OF PROVISION OF THE ACTIVITY

The place of fulfillment of SIGNICAT SLU's obligations regarding digital certification services and, where appropriate, software use licenses, is the registered address of SIGNICAT SLU.

5.2. SEVERABILITY OF THE TERMS AND CONDITIONS

The clauses of this document are independent of each other, for which reason, if any clause is considered invalid or unenforceable, the rest of the clauses will continue to be applicable, unless expressly agreed otherwise by the parties.

5.3. APPLICABLE REGULATIONS AND COMPETENT JURISDICTION.

Relations with SIGNICAT SLU will be governed by the provisions of Regulation (EU) 910/2014 eIDAS, by Spanish law, and especially by all those which arise from its compliance policy.

The competent jurisdiction is the one indicated in Law 1/2000, dated January 7th, on Civil Procedure, except where the APPLICANT/SUBSCRIBER is considered a consumer, in which case SIGNICAT SLU will submit to the jurisdiction that legally corresponds to it.