WISE SECURITY
a vargroup company

ERDS MEE

Certified Electronic Delivery Service Practice Statement

Classification: Public use

CONTROL DE VERSIONES			
Versión	Fecha de emisión	Cambios/Observaciones	Aprobado por
1.0	03/02/2021	Initial review	Óscar Flor Lozano
1.1	16/01/2023	Periodic review. Unchanged	Óscar Flor Lozano
1.2	22/01/2024	Periodic review. Unchanged	Óscar Flor Lozano
1.3	19/03/2024	Style change to VarGroup	Óscar Flor Lozano
1.4	25/03/2024	Add Camerfirma in point 2.6 Intervening Qualified Trust Service Providers. Delete reference to the "Terms and Conditions" document in point 9 TIME REFERENCES	Óscar Flor Lozano
1.5	15/04/2024	Update items 8.1, 10.5 and 18.1	Óscar Flor Lozano
1.6	13/01/2025	Periodic review. Unchanged	Óscar Flor Lozano
OID: 1.3.6.1.4.1.56976.1.1.1.1			

1 INTRODUCTION

Wise Security Global ("WSG") is an expert in cybersecurity, digital signatures and electronic certification whose mission is to protect its clients' business by creating trusted and secure electronic environments that enable them to maintain and enhance the trust of their stakeholders.

WSG is a Trusted Service provider in accordance with eIDAS 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 and Law 6/2020 of 11 November regulating certain aspects of electronic trust services.

This Certification Practice Statement details the general rules and conditions provided by WSG in relation to the Certified Electronic Delivery Service, the applicable conditions for the identification and authentication of the sender and receiver, the organisational and technical security measures, the integrity of the transactions, the accuracy of the date and time of sending and receiving data proving that such event has occurred, and the storage and custody of all evidence generated in the process.Â Â
This Certified Electronic Delivery Service consists of the generation of a proof that accredits the sending of a document by a sender, its receipt or rejection by the addressee, as well as the time at which both occurred and, if applicable, the access/downloading of attached documentation with the main purpose of being able to be used in legal contexts.

The content of this Certification Practices Statement is made in compliance with current legislation and aligned with 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/C and in compliance with Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.

Therefore, this Certification Practice Statement constitutes the general compendium of standards applicable to the activity of WSG as a Qualified Trust Service Provider.

In addition, WSG follows the indications of the European Telecommunications Standards Institute (ETSI) standards, guided by the technical specifications of EN 319 401 (general requirements for trusted service providers), ETSI EN 319 521 "Policy and security requirements for Electronic Registered Delivery Service Providers" and ETSI EN 319 522 "Electronic Registered Delivery Services", and has been drafted in accordance with the RFC 3647 "Certificate Policy and Certification Practices Framework" proposed by the Network Working Group for this type of document.

2 SERVICE USER COMMUNITY

2.1 Trusted service provider

The provider of the trust service defined under this Statement of Practice is Wise Security Global:

Wise Security Global SL
B-95732087
Alameda Recalde 34
48009 Bilbao
Contact: info@wsg127.com

2.2 Issuer

The sender is any natural or legal person who issues a communication and makes it available to an addressee through WSG's certified electronic delivery service. This sender must be previously identified by WSG, so that WSG can confirm with a high level of confidence that this person is who he/she claims to be.

In the case of qualified certified electronic delivery service, the issuer shall always be authenticated by an electronic certificate issued by a Qualified Trust Service Provider.

2.3 Recipient

The recipient is understood to be the natural or legal person to whom the communication sent by the sender is addressed, and which will be delivered by WSG's certified electronic delivery service, after authentication.

In the case of the qualified certified electronic delivery service, the recipient of the communication shall always be authenticated by means of an electronic certificate issued by a Qualified Trust Service Provider.

2.4 Identity Verification Officer

The Identity Verification Officer is the person who, on behalf of WSG, is entrusted with the function of verifying the initial identity of the sender and/or recipient. In the case of the qualified service, given that the authentication is always by qualified electronic certificate, it is not necessary to physically validate the identities.

2.5 Reliable third parties

Reliable third parties are those parties who rely on the services provided by WSG.

These third parties must take into account the limitations of the service, as well as be aware of the terms and conditions of the service. Specifically, third parties must check

the authenticity and integrity of the document, verifying the validity of the signature included in the final document, and that it is certified by WSG as a Trusted Service Provider, as well as that the digital certificate used for the signature was valid at the time of signing, and that the document remains intact and has not been modified.Â To do this, you can use programmes such as ADOBE, which validates the PDF document, or VALIDe, or any other programme that performs this verification.

Likewise, the document incorporates two time stamps, the first certifies that the document exists at the time of signing, and the second ensures that the evidence of revocation incorporated in the signature itself is durable over time, thereby generating a signature in PAdES LTV format, so that its long-term validity can be verified. In the event that the validity checking program reports that there is a problem with the signature (because the certificate has expired), the validity of the certificate can be checked at the time of signature since the revocation information was added in "Certificate details".

However, WSG will resolve any doubts related to the electronic trust service and the validity of the final document. To this end, any interested party may write to info@wsg127.com, requesting verification of the validity of the final document.

2.6 Intervening Qualified Trust Service Providers

List of Qualified Trust Service Providers involved in the qualified electronic certified delivery service is as follows:

- CAMERFIRMA: issuer of the company seal certificate, which is used to sign the certified electronic delivery service evidence.

- IVNOSYS: custodian of the previous company seal certificate, this certificate is hosted in an HSM.
  It is also an issuer of time stamps which are used to record the date and time of events occurring in the electronic registered delivery service.

- IZENPE: issuer of the time stamps used to record the date and time of events occurring in the electronic registered delivery Service.

3 DEFINITIONS AND ACRONYMS

3.1 Definitions

- **Certified electronic delivery user agent/application**: A system consisting of software and/or hardware components through which senders and recipients participate in the exchange of data with certified electronic delivery service providers.
- **Authentication**: The electronic process that makes possible the identification of a natural or legal person, or of the origin and integrity of data in electronic form.
- **Qualified Certificate**: Certificate issued by a Qualified Trust Service Provider and which meets the requirements set out in Annex I of EU Regulation 910/2014 (eIDAS) and which meets the requirements set out in Article 7 of Law 6/2020 (LSEC) regarding the verification of the identity and other circumstances of the applicants, and the reliability and guarantees of the trust services they provide, in accordance with Title III of the aforementioned Law 6/2020 LSEC .
- **Encryption**: Operation by which a clear message is transformed into an unreadable message.
- **User content**: Original data produced by the sender to be delivered to the recipient.
- **Consignment**: the act of making the user's content available to the recipient, within the limits of the electronic registered delivery service.
- **Cryptography**: The science of altering the original text so that the meaning of the message can only be understood by the intended recipient.
- **Delivery**: the act of successfully crossing the barrier of the recipient's certified electronic delivery service via the recipient's electronic delivery agent/application.
- **Sending**: the act of making the user content available to the recipient, within the limits of the certified electronic delivery service.
- **Event**: Relevant step in an electronic delivery process that can be supported by evidence of the certified electronic delivery service.
- **Evidence**: Data generated by the certified electronic delivery service that aims to prove that a certain event has occurred at a certain time.
- **Fingerprint**: The fingerprint is the alphanumeric code obtained after hashing a document. It is sometimes also referred to as a "unique digest" or "hash".
- **Identification**: The process by which a person proves his or her identity.

- **Content integrity**: Content integrity refers to any document or set of data that has not been changed or altered after signature.
- **Trusted Service Provider**: a natural or legal person who provides one or more trust services, either as a qualified provider or as an unqualified provider of trust services.
- **Certified Electronic Delivery Service Provider**: trusted service provider providing the certified electronic delivery service.
- **Qualified Electronic Certified Delivery Service Provider**: Service provider providing qualified electronic certified delivery services.
- **Repudiation**: From the sender's point of view, repudiation of the message means denying having sent it. From the addressee's point of view, denying having received it.
- **Electronic timestamp**: data in electronic format linking other data in electronic format to a specific point in time, providing evidence that the latter data existed at that point in time
- **Certified electronic delivery service**: a service that enables data to be transmitted between third parties by electronic means and provides evidence related to the handling of the transmitted data, including proof of sending and receiving the data, and that protects the transmitted data against the risks of loss, theft, damage or unauthorised alteration.
- **Qualified electronic certified delivery service**: a certified electronic delivery service that meets the requirements set out in Article 44 of Regulation 910/2014, eIDAS.
- **Handover**: the act of getting the user's content successfully across the edge of the certified electronic delivery service to the recipient's Application.
- **User**: natural or legal persons using certified electronic delivery services provided by WSG.

3.2 Acronyms

- **DPC**: Data Processing Centre.
- **CPD**: Certification Practice Statement.
- **eIDAS**: Regulation 910/2014 of the 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 1999/937/EC.
- **LSEC**: Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- **ERD**: A relevant step in the electronic delivery process that can be attested by evidence of service.

- **ERDS**: stands for Electronic Registered Delivery Service. It is the electronic service provided which can transmit data between third parties by electronic means providing evidence related to the management of the data and which protects the transmitted data against the risk of loss, theft, damage or any unauthorised alteration.
- **ERDSP**: Electronic Registered Delivery Service Provider.
- **ERD-UA**: Certified Electronic Delivery User Agent/Application.
- **OTP**: One-Time Password
- **ISMS**: Information Security Management System.
- **TSP**: Trust Service Provider. Trust Service Provider.

4 COMPLIANCE REQUIREMENTS

WSG declares that this Statement of Practice is applicable to the Qualified Electronic Certified Delivery Service complying with the requirements set out by Regulation (EU) 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 (eIDAS).

WSG guarantees, in accordance with legal and regulatory requirements, that:

- It complies with its Information Security Policy, which is in force and aligned with the applicable legal regulations.
- Complies with its Qualified Certified Electronic Delivery Service policy as defined in this Statement of Practice.
- Meets the organisational requirements as defined in point 5 of this Declaration of Practice.
- This CPD conforms to ETSI EN 319 521 "Policy and security requirements for Electronic Registered Delivery Service Providers, and controls have been implemented that meet the requirements specified by this ETSI standard, as well as ETSI EN 319 401, as a Trusted Electronic Service Provider.

5 OBLIGATIONS OF THE PARTIES

5.1 Obligations of the service provider

WSG, acting as a Certified Electronic Delivery Service Provider undertakes to:

- Comply with the provisions of this Qualified Electronic Certified Delivery Service Statement of Practice.
- Ensure the protection of your private keys of your certificates in a secure way.
- Manage the Certified Electronic Delivery Service according to the information sent by the customer and free of data delivery errors.
- Use appropriate means for the collection of evidence resulting from the service.
- Custody of the evidence issued to customers who contract the Qualified Electronic Certified Delivery Service.
- Inform the service subscriber of the characteristics of the service provision, the obligations assumed and the limits of liability.
- Publish this Qualified Electronic Certified Delivery Service Practice Statement, and keep it up to date.
- Use appropriate technologies and equipment, and have trained personnel to carry out their functions.
- In case of non-availability of the service due to maintenance, improvement or modification work, please inform your customers in good time.
- In the event of an incident in the service, immediately notify the parties involved who are or may be affected.
- Use qualified time stamps to ensure that events occurring in the service operate in sync with reliable time sources.
- Ensure the integrity, confidentiality and availability of user content, within WSG's certified electronic delivery service.
- Establish custody mechanisms for the evidence produced by the ERDS, protecting it from unauthorised tampering, falsification, loss, or destruction.
- To deal with requests, queries, complaints and claims from customers and third parties within a reasonable period of time. Complaints and suggestions can be submitted by filling in a form on the following website: https://erds-mee.com/quejas-y-sugerencias/
- Retain the information relating to the services provided for 15 years from the end of the service provided and, in any case, for the period established by the legislation in force.

- Notify the Supervisory Body of any substantial modification to this CPS. If the modification affects the parties concerned, they shall also be informed.
- Notify the Supervisory Body, within 24 hours, of the security breach with a significant impact on the trusted electronic service. Likewise, if the breach affects personal data, the Spanish Data Protection Agency shall be notified within 72 hours of becoming aware of it.

5.2 Obligations of customers/subscribers of the services

WSG clients undertake to:

- Be informed of the provisions of this Certification Practice Statement.
- Use the appropriate means for requesting services.
- Limit and adapt the use of the evidence resulting from the service to what is allowed by this CPD.
- To know and accept the conditions and limitations of use of the service that have been established in this CPS.
- Be aware of the provisions of this CPS, accepting and subjecting themselves to the provisions of this CPS and, in particular, to the responsibilities applicable to their acceptance and use of the services provided by WSG, as well as the evidence resulting therefrom.
- To notify, without delay, any failure, event or anomalous situation related to the services offered by WSG on this service.

5.3 Obligations of third parties

Persons, whether natural or legal persons, who rely on the certified electronic delivery service provided by WSG are obliged to:

- Be aware of the limitations of use (if any) of the service, according to this CPS and the terms and conditions of Service.
- Comply with the provisions of the applicable regulations.
- Report to WSG any incident related to the service as soon as they are aware of it and as soon as possible.
- Verify the validity of the electronic signatures or seal used to sign the certified evidence document.

5.4 Obligations of WSG providers

WSG providers whose services have an impact on the certified electronic delivery service provided by WSG, such as providers of qualified certificates for the signing of evidence and providers of time-stamping service shall:

- Ensure that qualified certificates issued in the name of WSG and certificates issuing time-stamp tokens remain qualified.
- Communicate to WSG any change in their status as a qualified person.

6 INTEGRITY AND CONFIDENTIALITY OF USER CONTENT

WSG uses a qualified E-Stamp certificate issued by Camerfirma, a Qualified Certification Service Provider, which is installed on IvSign plataform in the Ivnosy's HSM, guarantees the adequate availability, integrity and confidentiality of the user's content when using this service.

WSG guarantees the confidentiality of the identity of the sender and the recipient, both during sending and during the custody of the evidence by encrypting communications using robust algorithms (TLS with RSA and AES minimum 128 bits and CBC mode, SHA minimum 256 bits).

One or the other algorithm is used depending on the cryptographic capabilities of the connected client's browser (the strongest algorithm within the client's capabilities will be used), in all cases the TLS protocol version is 1.3 and the asymmetric keys are 2048 bits.

This list of permitted algorithms is configurable, allowing the system to be more or less restrictive in this respect; however, it will never be served under an algorithm lower than those listed. The list is updated according to the security directives in force.

The certificate that will serve the protocol is a qualified website authentication certificate requested by Wise Security Global, and issued by a Qualified Trust Service Provider.

WSG guarantees the integrity of the content and its associated metadata, both during transmission from sender to recipient and between the components of the distributed system of the Service, as well as during storage, duly preserved for 15 years and until the statute of limitations for possible legal action, by means of a digital signature supported by a qualified certificate generated by a Qualified Certification Service Provider, and incorporating a qualified time stamp, in such a way as to exclude the possibility that the data may change in an undetectable manner.

The system will never modify the user's content, not even for formatting changes, the content will be entirely what the sender has created.

Up to 3 files may be attached to each submission in PDF format only, with a maximum size of 5MB each.

7 IDENTIFICATION AND AUTHENTICATION IN THE SERVICE

7.1 Initial identification of the parties

The identity of both the sender and the receiver is verified on the basis of their valid electronic certificate, issued by a Provider included in the List of Trusted Service Providers of the Ministry responsible for trusted electronic services.

This verification is performed each time the user accesses the ERDS MEE service, so that it is guaranteed that the validity period allowed for a single certificate may not exceed a maximum period of 5 years from the first identification, the maximum validity periods established by the different PSCs in no case approach 5 years, and in each authentication the expiry of the certificate is verified, as well as its revocation status.

7.2 Authentication

As a method of authentication in the qualified service of certified electronic delivery, both the sender and the recipient must use certificates of a natural person or of a legal representative of a legal person, issued by a Qualified Trust Service Provider.

7.3 Recipient identification and user content delivery

WSG will deliver the user content to the recipient only after successful identification of the recipient. The identification of the recipient is based on a certificate of a natural person or legal representative of a legal person, issued by a Qualified Trust Service Provider. WSG's certified electronic delivery service platform will perform the prior verification of its validity, before making the user's content available to the recipient.

8 EVENTS AND EVIDENCE

8.1 Event registration

WSG shall keep a log of service events, storing at least the following:

- Sender and recipient identification data, including events and identity verification information
- Sender and recipient authentication data, including events and authenticity verification information.
- Proof that the identity of the issuer has been initially verified, if applicable.
- Transaction records, verification of identity of sender and recipient, and communication.
- Proof of recipient's identity verification before sending/transferring user content.
- Proof that the user content has not been modified during transmission. Such proof shall be provided by the inclusion of a WSG entity stamp and time stamping.
- A reference or a complete compilation of the submitted user content.
- Time-stamp tokens corresponding to the date and time of dispatch, consignment and delivery, as appropriate.

The evidence produced by the service shall be made available to the parties in PDF format. These files shall be electronically signed in PAdES format and these signatures shall be stamped by a qualified electronic time stamp. The signatures will self-contain all the revocation check information of the certificates involved in the signature, and will have a second time stamp that seals this content, all following the requirements defined in the ETSI EN 319 142-1, in accordance with the implementation decision (EU) 2015/1506 of the Commission on 8 September 2015, establishing specifications for advanced electronic signature formats and advanced electronic seals according to the eIDAS Regulation, generating signature in PAdES LTV format.

8.2 Monitoring frequency

Audit trails are periodically reviewed for suspicious or malicious activity. Actions taken after the audit must be fully accessible and documented. The processing of audit logs consists of a review of the logs including verification that the logs have not been tampered with, a brief inspection of all log entries and further investigation of any alerts or irregularities.

8.3 Retention period and validity

WSG will retain all records for a minimum of 2 years according to the requirement REQ-ERDSP-7.10-02 of EN 319 521.

However, the evidence produced by the service and included in the final Declaration will be retained by WSG for 15 years.

8.4 Events recorded by the service

8.4.1 Electronic Certified Delivery Service events recorded at source

- **A.1 SubmissionAcceptance**:
  Acceptance of the sending: It is evidenced that the sender, duly identified, as can be proved with the information of the identification data and verification of the identity of the sender, at a given moment has successfully submitted the content of the notification to WSG's certified electronic delivery service, and WSG has accepted it, and in turn, has tried to deliver it to the recipient of the same.
  At the functional level, this evidence is produced when, in the Issuer Portal, the issuer user clicks on the Submit button in the notification registration form.
  Status of the minutes reached: Sent

8.4.2 Recipient notification events

- **C.1 NotificationForAcceptance:**
  Notification of sending to the addressee for acceptance: Evidence is produced that WSG sent a notification to the addressee, at a given time, communicating the availability of a message sent by the sender and requesting its acceptance.

  At the functional level, this evidence is produced immediately after A.1 SubmissionAcceptance, as part of the process triggered by the submission.

  Status of the minutes reached: Sent

- **C.2 NotificationForAcceptanceFailure:**
  Failure of notification for acceptance: Evidence is produced that the recipient could not be notified of the availability of the content of the notification due to technical errors. Related evidence attests that a notification requesting acceptance of a message could not be sent to the specified addressee.
  At the functional level, this evidence is produced when the mail server configured to send the email notification returns a response that the email could

not be delivered to the recipient, for example because the email address provided by the sender does not exist.
Record status reached: Unsuccessful submission

8.4.3 Acceptance or rejection events of user content by recipient

- **C.3 ConsignmentAcceptance:**
  Acceptance of the notification: there is evidence that the addressee, duly identified, took an explicit action indicating to the ERDS that it accepts to receive the content of the notification sent by the sender.

  At a functional level, this evidence is produced when the user clicks on the link that arrives in the notification email, and this link takes him to a window where he can accept or reject, this evidence is generated in the case of acceptance.

  Status of the minutes reached: Made available

- **C.4 ConsignmentRejection:**
  Rejection of the notification: there is evidence that the addressee, duly identified, took an explicit action indicating to the ERDS that he/she refuses to receive the content of the notification sent by the sender.

  At a functional level, this evidence is produced when the user clicks on the link that arrives in the notification email, and this link takes him to a window where he can accept or reject, and this evidence is generated in the case of rejection.

  Status of the minutes reached: Rejected

- **C.5 AcceptanceRejectionExpiry:**
  Expiry of acceptance/rejection: WSG's certified electronic delivery service sent a notification to the recipient, but the recipient did not respond to the notification with an acceptance/rejection. That is, it is evident that the recipient has not taken any action to accept or reject the user's content, after a certain period of time according to the applicable policies.

  At the functional level, this evidence occurs when, after 10 days from the date of sending the e-mail to the addressee, there has been no acceptance or rejection of the notification.

  Status of the act reached: Expired

8.4.4 User content delivery events to the recipient

- **D.1 ContentConsignment:**
  Content of the notification: the content of the notification itself is evidenced by the date on which it is made available to the addressee.

  Status of the minutes reached: Made available

- **E.1 ContentHandover:**
  Delivery of user content to the addressee: Evidence that the content of the notification has successfully passed the border of the certified electronic delivery service and is successfully delivered to the addressee, after authentication.

  The event will indicate a "PULL", i.e. the recipient proactively requests the download of the content.

  At the functional level, this evidence is produced when, in the Recipient Portal, the recipient user clicks on the Detail button in the list of his or her notifications.

  Status of the minutes reached: Delivered

All such evidence is retained by WSG and incorporated into the PDF document issued and stamped by WSG with a qualified electronic seal certificate and a time stamp. This document will remain available to the parties and interested third parties for the entire retention period. In order to obtain an electronic copy of the document, the interested party can download it at any time from the ERDS MEE issuing and receiving portals.

9 TIME REFERENCES

The time references set out in each of the events of the Electronic Certified Delivery Service, in particular:

The date and time of sending the user's content by the sender to WSG's certified electronic delivery service and of receipt by the recipient shall be indicated by means of a qualified electronic time stamp, issued by Ivnosys or Izenpe; both are Qualified Time Stamp Service Providers.

Proof of sending and proof of receipt are linked to the user's content and stamped with a qualified time stamp.

WSG shall verify, at least once a year, that the Time Stamp Service Providers used continue to be qualified by performing an interpretation of the TSL as indicated by the European Commission.

10 PHYSICAL SECURITY, MANAGEMENT AND OPERATIONS

10.1 Physical security controls

WSG warrants that it fully complies with applicable law in all aspects of physical security as described throughout this document and in its internal procedures.

In order to fulfil the service, different centres where critical or sensitive activities are carried out have been established with appropriate security barriers and entry controls with security control mechanisms in place to reduce the risk of unauthorised access or damage to IT resources.

Location of facilities

All the facilities where the service is offered have security measures for access control so that the development of the activity, as well as the provision of services, are carried out with sufficient guarantees of confidentiality and security.

In order to guarantee the security and continuity of services, WSG has an infrastructure based on Public Cloud providers that offer a hosting service. It provides a network architecture and a data centre designed to meet the most demanding security requirements, with adequate levels of protection and security. The provider where the production servers that provide the service are hosted has the most relevant security certifications.

Physical security measures

The following are, by way of example, some of the security measures for the provision of the service:

Physical access

- The buildings have physical access control and perimeter security measures in place, consisting of different rings with adequate technical and human resources to guarantee the security of the facilities.

  In addition to external perimeter security, there are various means of internal control, rooms and installations protected by CCTV, intrusion detectors, access control, fire detectors, etc.
- There is an exhaustive system of physical control of people at the entrance to the building.
- All critical operations are carried out in a closed and controlled environment with additional security measures.

Electricity and air conditioning

- The rooms where the machines of the service infrastructure are located are supplied with electricity and air conditioning, creating a reliable operating environment. In addition, the system is protected against voltage drops or any other anomaly, as the system is redundant with a double electrical supply.
- In the case of AWS, it offers power supply systems designed so that they can be fully duplicated and maintained without impacting operations, 24 hours a day.
- Similarly, heat and humidity control mechanisms and liquid probes have been installed to achieve full and correct operation.
- Cabling safety: the cabling is located in a false floor or ceiling and has adequate means of protection.

Fire prevention and protection

- The rooms have adequate means (fire detection and extinguishing equipment) to protect the contents of the rooms.

Media storage and backup/restoration

- Backups are also performed in the hosting providers' environments and a backup log is available for possible emergency restoration.
- There are contingency plans for the service that WSG manages, all aimed at preserving business continuity in the event of any anomaly.

Physical location of service maintenance personnel

All ERDS MEE services are provided 100% from the environments of the hosting providers contracted for this purpose, the physical location of these environments, as well as all the security measures described are the responsibility of these providers.

WSG personnel performing service maintenance work operate from different WSG physical offices, which have their own physical security measures in place.

WSG has a procedure called "***ERDS_MEE_2.18._Physical_and_environmental_security***" which contains a detailed list of the physical measures that have been implemented both at WSG and at the providers of hosting services, in order to protect the facilities from unauthorised access and from damage caused by natural disasters or environmental phenomena.

10.2 Logical security controls

WSG employees shall only have access to the information systems of the certified electronic delivery service according to their profile and to such information as is necessary for the performance of their duties.

Data concerning this section is considered confidential information and is only provided to those with a need to know, such as in the case of external or internal audits or inspections by authorised authorities.

WSG has a procedure called "**ERDS_MEE_2.21._Logical_access_control**" which contains detailed information on logical security.

10.3 Computer security assessment

WSG continuously evaluates its security level in order to identify possible weaknesses and establish corrective actions through internal and external audits as well as regular security checks.

10.4 Life cycle security controls

WSG periodically commissions a review of all its systems and applications involved in the management of the service.

10.5 Acquisition controls and systems development

WSG is in charge of positioning the level of security required both in the acquisition and in the testing and development of computer systems that may have an impact on the service it provides. There is a specific procedure that regulates this.

The review of systems configuration takes place on an least annual basis, or when there is any relevant change that affects it..

11 PRIVACY AND DATA PROTECTION

In compliance with the requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, "**GDPR**") and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights (hereinafter, "**LOPDGDD**") WSG is committed to respecting the privacy and protection of data subjects' data, in accordance with the aforementioned regulations, its Privacy Policy and the Terms and Conditions of Service. In this regard, WSG has a Register of Personal Data Processing Activities which includes the processing necessary for the provision and management of the Certified Electronic Delivery Service.

In accordance with the above, the user is informed of the following aspects related to the processing of data derived from the provision of the Certified Electronic Delivery Service:

WSG (WISE SECURITY GLOBAL, S.L.), with postal address Alameda Recalde 34, 48009 Bilbao (SPAIN) telephone +34 910 700 549, will process the data for the purpose of providing the requested service under the terms established in current legislation, in this CPS and, where appropriate, in the Terms and Conditions reached between the participants and WSG.

Apart from the purposes mentioned in the previous section, no other data processing will be carried out, unless the user is previously informed and his or her consent is obtained or a regulation allows the intended processing.

WSG is committed to assisting the user in relation to exercising rights, communicating a data breach, assessing the impact of the processing or making prior enquiries to the Supervisory Authority.

On the other hand, where there is a prior contractual relationship with WSG, the latter may send the user commercial communications by e-mail provided that they refer to products or services similar to those that were initially contracted. In each of the commercial communications that are sent in this way, the recipient will be offered the possibility of opposing the processing for this purpose in a simple and free manner.

The interested user may exercise the rights of access, rectification, opposition, suppression, limitation of processing and portability of personal data, requesting it by email to the email address legal@wsg127.com or by post, at the address indicated

above, accompanied by an identity document. However, if the data subject believes that his or her right may have been infringed, he or she may file a complaint with the Spanish Data Protection Agency.

WSG has adopted all the necessary technical and organisational measures to guarantee the security of the data being processed and to avoid its loss, theft, modification, alteration or unauthorised access.

The measures implemented depend on the nature of the data managed and the level of security which, for this reason, is applicable to them. The set of security measures implemented shall be a consequence of the current state of technology and shall be adapted as technology evolves.

WSG undertakes to process the data only for the purpose for which they were collected. When collecting personal data, the data subjects will be informed of the mandatory or optional nature of the responses. Only data which, in accordance with the principle of quality, are adequate, relevant and not excessive in relation to the purpose for which they were collected, must be provided. For this reason, refusal to provide such data will make it impossible to provide the service.

The user undertakes to ensure that all information provided is accurate and truthful. Likewise, he/she must immediately inform us of any update that needs to be made or any error or inaccuracy that he/she detects.

On the other hand, the personal data provided directly by the interested party or by third parties will form part of a file under the responsibility of WSG for the purpose of managing and maintaining the contacts and relationships that arise as a result of the relationship with WSG. The legal basis that legitimises this processing will be the need to manage a contractual or similar relationship.

They must only be used for the purpose for which they are intended and may not be passed on to third parties. The period of retention of this data will be determined by the relationship between the data subject and WSG.

Personal data shall not be transferred or communicated to third parties without the prior consent of the data subject, except for those transfers that must be carried out due to legal obligation, for example, they may be communicated to the Ombudsman, the Public Prosecutor's Office or the Judges or Courts or the Court of Auditors, in the

exercise of the functions attributed to them or to autonomous institutions with similar functions to the Ombudsman or the Public Prosecutor's Office.

WSG, within the framework of the provision of the service with the Client, will process the data only upon documented instructions from the Client (who will act as Data Controller), and will in any case take appropriate technical and organisational measures to ensure that the processing complies with the legal requirements, in particular by ensuring a level of security appropriate to the risk, the protection of the rights of data subjects, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons, including:

- Pseudonymisation and encryption of personal data.
- The ability to ensure the continued confidentiality, integrity, availability and resilience of systems and processing services.
- The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, evaluating and assessing the effectiveness of technical and organisational measures to ensure the security of processing.

For further information regarding the data processing carried out by WSG, the data subject may contact WSG by sending a letter to the following address:

Alameda Recalde 34

48009 Bilbao

or by e-mail to the WSG Data Protection Officer (dpo@wsg127.com), enclosing the documents required by law.

Likewise, WSG personnel have a duty of confidentiality with regard to the information they handle in the course of their work. Information classified as "confidential" shall under no circumstances be disclosed to third parties, except in cases of collaboration with the competent authorities and institutions.

Information which has not been expressly and generally declared as public shall be deemed to be confidential:

- Contingency and business continuity plans.
- Information relating to the operation and maintenance of the service.

- Information relating to control parameters. Security and audit procedures.
- Personal data information provided to WSG during the registration process of subscribers to the service.
- Business-related information.
- Transaction logs, full logs and log records.
- In general, everything classified as "CONFIDENTIAL".

It shall also be considered as public information:

- This Certification Practices Statement of the Certified Electronic Delivery Service.
- The Terms and Conditions of Service.
- WSG Privacy Policy.
- All information that has been classified as "PUBLIC".

12 TRUSTED ROLES

Trust roles are statuses referring to the degree of security or the assignment of certain tasks by someone empowered and authorised to do so.

These roles include:

- System Administrator: System Administrators are authorised to configure, install and maintain WSG's trusted systems for service management including system recovery.
- System Operator: They are responsible for operating the WSG systems on a regular basis. Their functions deal with general operation and backup.
- Internal auditor: He/she will be authorised to view files as well as to audit the logs of WSG's trusted systems. He/she shall be responsible for checking the tracking of incidents and events, the protection of systems, as well as checking alarms and physical security elements.
- Security officer: The security officer is responsible for the administration of the implementation of security practices and security procedures, both physically and logically. He/she should be responsible for verifying that all documentation is accessible when required and correctly numbered, as well as for checking the consistency of documentation with procedures, inventoried assets, etc.
- Service Manager: will be responsible for the maintenance and management of WSG's certified electronic delivery service, in such a way that all technical and operational requirements that are incorporated in the applicable standards are implemented. Likewise, he/she is in charge of all security aspects related to the service, and will manage them jointly with the Security Manager.

13 COMPLIANCE AUDITS

All tools, reports or records, files and sources related to the preparation or recording of an audit are considered confidential and sensitive information and as such are treated in all aspects and access to them is restricted to authorised persons.

13.1 Audits frequency

Periodically, corresponding audit plans will be drawn up, which will include as a minimum a review of:

- The present CPD and service policies in force.
- Security policy.
- Physical security of the facilities of the audited service.
- Logical security of WSG's certified electronic delivery service systems.
- Technological assessment of service components.
- Administration of the services, as well as security in the same.
- Compliance with applicable legal requirements.

The qualified electronic certified delivery service included in this FAD is subject to periodic audits, as dictated by the relevant certification scheme, related to the European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

This audit shall be carried out annually by an external company that is duly accredited.

Each of the Qualified Trust Services provided by WSG will be audited in accordance with the relevant scheme, and this is stated in the relevant Statement of Practice for that service.

13.2 Auditor qualification

The auditor who verifies and verifies the correct operation of WSG shall be a person with sufficient official qualifications, as well as adequate and demonstrable experience in the subject matter to be audited, in accordance with the legislation in force at any given time.

The name and identification of the auditors shall always appear together with the report obtained during the audit, and the report shall be signed by the auditors and by the head of the audited entity.

13.3 Auditor relationship with the audited company

The performance of audits may be entrusted either to External Audit Firms or to qualified internal personnel, in accordance with the legislation in force in this respect, or both. In the case of internal personnel and, similarly, depending on the level of criticality of the area or system to be audited, the degree of independence of such personnel, as well as their level of experience, shall be determined on a case-by-case basis, in accordance with functional independence parameters.

In cases where audits are conducted by personnel external to WSG, additional measures and controls will be put in place to ensure that audit requirements are rigorously complied with. In addition, access to sensitive information and other confidentiality and liability agreements will be signed.

In external audits, the auditor, as well as the auditing company, will never have any type of labour, commercial or other type of relationship with WSG, nor with the party requesting the audit, being always a totally independent professional who carries out the requested audit.

In the case of the audit of the certified electronic delivery service in order to be considered a qualified service in accordance with eIDAS, this audit must be carried out by an external company that is duly approved for the performance of the audit.

13.4 Audit results communication

Independent administrative or judicial authorities may request audit reports to verify the proper functioning of the platform.

The result of the audit of the eIDAS compliance assessment for the WSG electronic certified delivery service to be considered as a qualified service will be submitted to the supervisory body in Spain for the granting or, as the case may be, maintenance of such qualification.

14 CONDITIONS AND GUARANTEES OF USE

The certified electronic delivery service will always be performed in accordance with the function and purpose set out in this Statement of Practice for the Certified Electronic Delivery Service, the Terms and Conditions of Service and in accordance with the applicable regulations.

The Qualified Electronic Certified Delivery Service provides the secure and reliable delivery of electronic messages between the parties involved by producing an evidence in the delivery process which allows for a certification of the fact on a legal level. Thus, the evidence can be seen as a statement from a reliable party that a specific event related to the delivery process occurred at a specific time.

Service availability

WSG's Qualified Electronic Certified Delivery service will be available 24 hours a day, 7 days a week. Availability is the ability to access the service on demand, regardless of its speed. The availability to which WSG commits will be reflected in a Service Level Agreement signed with each of its customers.

The period within which the addressee can dispose of the content of the notification is 10 (ten) days. After this period, the message will no longer be available for receipt by the addressee.

Parties relying on this certified electronic delivery service may obtain information about the service by sending an email to info@wsg127.com. In providing the services described in this CPS, WSG warrants that it will not operate in such a way as to engage in any discriminatory practices.

A contingency procedure is in place that defines the actions to be taken, resources to be used and personnel to be employed in the event of an intentional or accidental event that disables or degrades the resources and certification services provided by WSG.

Without prejudice to the security measures applied, the policy, procedure and controls for Business Continuity management are defined in the procedure "**ERDS_MEE_2.16.Management of the service continuity plan**".

The objective of this procedure is to establish the guidelines for the contingency strategy in the event of incidents or disasters in the systems that support WSG's business processes. This procedure includes plans, instructions and measures that enable the continuity or restoration of the operability of information systems in the event of an incident or disaster.

System continuity generally includes one or more of the following approaches to restore disrupted services:

- Restoring operations at an alternative location.
- Recover operations using alternative systems.
- Execution of some or all affected business processes using manual means (no ICT systems). This option is only acceptable for very short interruptions.
- Adoption of incident and disaster prevention measures.

14.1 Economic conditions

The rates applicable to certified electronic delivery services, under the conditions set out in this CPS, will be provided to clients or potential clients by the WSG Sales Department. The price for the provision of the service under special conditions will be agreed in each case with the client and will be stated in the corresponding contract.

They shall apply only to the sender of the communication, this being a free service for the addressees.

WSG may, however, establish contractual frameworks with individual customers that particularise these conditions for the collaboration scenario established between the two parties.

15 RESPONSIBILITIES

WSG, as a Trusted Service Provider, is subject to the liability regime set out in article 13 of the eIDAS Regulation and 10 of Law 6/2020, regulating certain aspects of electronic trust services (LSEC) and will therefore assume liability for damages caused deliberately or through negligence to any natural or legal person, under the terms set out in the legislation in force.

To this end, and in compliance with the obligation of article 9.3.b) of the LSEC, WSG has taken out a civil liability insurance policy of two (2) million euros to cover the risk of civil liability for damages that may be caused by its failure to comply with the obligations imposed by the eIDAS Regulation.

15.1 Responsibility limitations

- WSG shall not be liable for damages caused by force majeure, unforeseeable or unforeseeable circumstances, or which could not have been foreseen and could not have been avoided.
- WSG shall not be liable for the acts or omissions made by the Client, and the Client shall be liable for all damages, direct and indirect, that may be caused to any person, property, company, public or private service, specifically for loss of profits, loss of information and data, or the corresponding damages, as a result of the acts, omissions or negligence of the Client, as well as of third parties linked to it, due to inappropriate, improper or fraudulent use, at the sole risk of the Client.
- WSG shall not be responsible for the content of the messages or documents sent.
- WSG is not liable for the negligence in the confidentiality and conservation of the access data to the service by the users of the ERDS.
- WSG shall also not be liable for damages if the recipient acts negligently. Among other cases, the recipient shall be deemed to have acted negligently if he fails to take into account the suspension, revocation or invalidity of the electronic certificate, or if he fails to verify the electronic signature or electronic seal.

16 TERMINATION OF SERVICE

In case of termination of the Qualified Electronic Certified Delivery Service, the following aspects must be taken into account, WSG has a Termination Plan, which takes into account the following aspects

16.1 Actions prior to the cessation of activity

In the event that WSG ceases to be a Trusted Service Provider, it shall give at least two months' notice, or as short a period of time as possible, to users and interested parties by means of a publication on the service website.

16.2 Communication at stakeholders and third parties

WSG will inform all customers, as well as entities with which there are agreements, contracts or other forms of relationship established, including trust practices, of the termination of the service by means of a service that proves the effective delivery and receipt of the communication, whenever feasible.

16.3 Notification to the supervisory body

WSG undertakes to notify the Ministry and competent authorities in the field of Trusted Electronic Services, within a maximum period of 3 months, of the cessation of its activity as a Trusted Service Provider, as well as of any other circumstance relevant to the cessation of activity.

16.4 Transfer of obligations

WSG undertakes to transfer its obligations to a trusted service provider to maintain and not to compromise, at any time, all necessary information on evidence, logs and events of operations for the period of time it has committed to, unless it can be demonstrated that WSG does not have such information.

WSG undertakes to collect all information and transfer it to a trusted service provider with whom it has an agreement to implement the Termination Plan in the event of bankruptcy.

In the event that it is not possible to carry out such a transfer or to agree on the transfer with another Trusted Service Provider, this information shall be forwarded to the Ministry responsible for Trusted Electronic Services.

Where there is a cessation of activity without bankruptcy, the information shall be stored appropriately.

16.5 Service keys management

WSG undertakes to destroy both the private keys and the backup copies, so that they cannot be recovered in any way. In the event that the private keys are managed by a Qualified Trust Service Provider, it will order the latter to revoke the certificate and destroy the private key.

16.6 Obligations by Wise Security Global, following the cessation of its activity

WSG has an agreement in place to cover operating costs to meet minimum operability requirements in the event of bankruptcy or for the reasons that it cannot cover the costs itself, in accordance with applicable bankruptcy law.

WSG, undertakes to maintain its obligations to make its public key available to trusted parties for the legally established period of time by fulfilling its obligations to do so.

17 APPLICABLE LAW

In the event of any dispute, WSG shall submit to the Courts of Spain for resolution, without prejudice to WSG's right to initiate legal proceedings before the courts of law of the Customer.

The implementing rules shall be as follows:

- 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 (eIDAS).
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (LSEC).
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting minimum technical specifications and procedures for security levels of electronic identification means in accordance with Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).
- Law 34/2002 on information society services and electronic commerce.

In addition, the following standards may apply:

- ETSI EN 319 521 "Policy and security requirements for Electronic Registered Delivery Service Providers".
- ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI). Electronic Registered Delivery Services. Part 1: Framework and Architecture".
- ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI). Electronic Registered Delivery Services. Part 2: Semantic content".
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI). General Policy Requirements for Trust Service Providers".

- ETSI EN 319 102-1 "Electronic Signatures and Infrastructures (ESI). Procedures for Creation and Validation of AdES Digital Signatures. Part1: Creation and Validation".
- ISO/IEC 29115: "Information Technology - Security techniques - Entity authentication assurance framework
- ISO/IEC 27001:2014. Information technology. Security techniques. Information security management systems. Requirements
- ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.
- NIST SP 800-63B "Digital Identity Guidelines Authentication an Lifecycle Management".

18 APPROVAL AND REVISION OF THIS DPC

18.1 DPC approval

The approval of this Certification Practice Statement is the responsibility of the Service Manager.

WSG has established a Cybersecurity Committee responsible for the implementation of the organisational and security policies and procedures necessary to ensure compliance with the requirements set out in this Certification Practice Statement.

Once approved, the CPD will be made public through publication on the WSG website.

18.2 DPC modification

This CPS may be amended for legal, technical or commercial reasons.

When the CPD is amended, it shall be notified to the Trusted Electronic Services Competent Body.

The latest approved version of the CPD shall be published on the WSG website.

Changes that may materially affect subscribers to the service or third parties will be notified by posting on the WSG website.

Changes that can be made to this CPD that do not require notification are stylistic or typographical corrections, editing changes or changes to contacts.

19 COMPLAINTS AND DISPUTE RESOLUTION

WSG will respond within a maximum of 30 days to any complaints that may be raised by users of the services. Such complaints must be sent in writing to the following email address info@wsg127.com

For any dispute that cannot be resolved amicably in relation to the provision of WSG services, users who are legal entities accept the jurisdiction and competence of the Courts and Tribunals of the City of Madrid, expressly waiving any other jurisdiction to which they may be entitled. With regard to claims brought by natural persons, the competent jurisdiction shall be the jurisdiction to which Spanish procedural legislation refers at any given time.

20 OTHER STIPULATIONS

Users of the WSG services referred to in this Statement of Practice accept the content of this document in its entirety. The declaration of invalidity of any of its sections shall not affect the validity of the remaining sections.