Framework Agreement of identification and authentication of users for access to the information systems of Enagás

Party of the first part, **ENAGÁS, S.A.** (hereinafter, “ENAGÁS”)

And party of the second part, **Company requesting access to the information systems of ENAGÁS, S.A.**, (hereinafter, SUBJECT)

For the purposes of this Agreement, ENAGÁS and SUBJECT shall be jointly referred to as the “Parties” and individually and indiscriminately as the “Party”.

Both parties recognise sufficient legal capacity to execute this Agreement.

RECITALS:

1 Whereas ENAGÁS provides strong authentication services based on two-factor technologies using security architecture and services based on leading systems in the sector.

2 Whereas ENAGÁS provides certification services pursuant to Law 59/2003, of 19 December, on the Electronic Signature. The electronic certificates issued shall comply with the technical specifications and shall be used for the purposes defined in the Declaration of Certification Practices published by ENAGÁS. The access path to this Declaration is included in the characteristics of the certificates issued.

3 Whereas SUBJECT is interested in using these strong authentication methods for access to the information systems managed by ENAGAS S.A. and/or its subsidiaries (or by ENAGÁS group companies).

By virtue of the foregoing, both Parties agree to execute this Framework Agreement for the provision of user ID services through the use of the software and architecture of services provided by ENAGÁS, in accordance with the following:

TERMS AND CONDITIONS

1. PURPOSE

The purpose of this Agreement is to enable ENAGÁS to provide SUBJECT with the user ID and authentication service through the use of the hardware and/or software proposed by ENAGÁS as a strong authentication mechanism, for access to the information systems of ENAGÁS, and the use of the services by SUBJECT, in accordance with the terms set out in this Agreement.

2. PUBLICATION OF THE AGREEMENT. ACCESSION DOCUMENT

This Agreement shall be published on the ENAGÁS corporate website and digitally signed by ENAGÁS for the purpose of electronically setting the publication date and guaranteeing the integrity of its content in any downloaded electronic copy. Any amendments to the text of the Agreement shall be duly reported to SUBJECT and included in the new version of the Agreement, which shall replace the previous one and shall be published as described above.

The Agreement shall be signed by ENAGÁS and SUBJECT through the electronic signing of the Document of Accession to the same.

3. OBLIGATIONS OF ENAGAS

3.1 ENAGÁS shall provide the hardware and/or software means necessary to proceed to the strong authentication and identification of users that access, on behalf of SUBJECT, the information systems of Enagás S.A. or any of the ENAGÁS group companies. The persons authorised to access the information systems of ENAGÁS in representation of SUBJECT are detailed in Appendix I of the Document of Accession to this Agreement. This appendix must be updated with the registrations and de-registrations of SUBJECT that take place.

Strong authentication mechanism refers to the mechanism which, to authenticate users, requires at least two different methods to be used at the same time, from among the following:

- Method based on something that is known. The knowledge of something that is known exclusively to the user is required. For example, password, numeric PIN, graphic pattern, etc.

- Method based on something that is owned. It is necessary to demonstrate something that only the user could have. For example, a credential (national ID document, passport), crypto token, an email address, a mobile telephone number, etc.

- Method based on something that is unique to the user. It is necessary to demonstrate that the user possesses a unique physiological quality. For example, fingerprint, facial recognition, recognition of the iris or retina, etc.

3.2 The strong authentication mechanisms that ENAGÁS implements at any given time shall be provided to users using telematic means providing this is possible. If a physical delivery is required, this will be sent to the address of the registered office of the company included in this agreement.

3.3 If electronic certificates are used, these shall be provided on a software support (file) or hardware support (cryptographic card, crypto token or the like) depending on the purpose and the technology available at the time of signing. The electronic certificate shall not be conditioned by the medium delivered.

For the purposes of this agreement, it shall be understood that a certificate of components is an electronic certificate issued by ENAGÁS that associates signature verification data to a computer app over which there is a specific legal entity that acts as controller, and this party holds control over said app.

3.4 The characteristics of use and security of the strong authentication mechanisms provided by Enagás are defined in accordance with the security standards of the series of ISO/IEC 27000 standards and defined in the Declaration of Certification Practices of ENAGÁS in the event of being a certificate.

3.5 At the request of SUBJECT, notified pursuant to Clause 10, ENAGÁS shall proceed to revoke and withdraw the access authorisation of those users designated in Appendix I as may be specified by SUBJECT. Similarly, ENAGÁS shall proceed to register those users who, in the same way, are notified by SUBJECT. The foregoing changes shall be implemented by updating Appendix I. This shall require the signing of a new Appendix I which shall extinguish and replace the one in force at the time of its novation.

3.6 Enagás reserves the right to block access or definitively remove users who because of prolonged inactivity, suspected phishing, suspicious behaviour or in general any reason that can be interpreted as a risk for the company's security. The changes shall be notified to the company's representative for clarification and consolidation in Appendix I of the Document of Accession of this Agreement.

4. OBLIGATIONS OF SUBJECT

4.1 SUBJECT shall furnish ENAGÁS with the data concerning the users of its company, for which access is requested.

4.2 SUBJECT shall collaborate with ENAGAS and keep the latter informed of all aspects that may be necessary for better development of the services under this Agreement. In particular, SUBJECT: (i) shall supply all the information and documentation required, being responsible for its truthfulness and accuracy; (ii) shall immediately notify ENAGÁS in the event of detecting that any wrong or inaccurate information has been included or in the event that, in an ensuing manner, the information identifying the user or of Appendix I does not correspond with reality; and (iii) shall request the suspension/revocation of user access and/or certificate from the ENAGÁS information systems whenever this party, for whatever reason, ceases to represent SUBJECT.

4.3 SUBJECT must be equipped with the required hardware and software infrastructure to access the system, in accordance with the specifications published on the Corporate Website of ENAGÁS www.enagas.es.

4.4 The strong authentication mechanisms are personal and non-transferable, and therefore SUBJECT cannot furnish this or assign any element whatsoever related to these mechanisms to persons other than those specified in Appendix I, nor these to any other person, whether an individual or legal entity.

4.5 SUBJECT undertakes to look after and use the electronic certificates diligently in accordance with the law and the limits set by the Declaration of certification practices published by ENAGÁS and the certificate itself.

4.6 SUBJECT undertakes to immediately notify ENAGÁS of the loss, theft, misappropriation, misuse or falsification of any element related to the strong authentication mechanism, requesting revocation of the same and, in general, with regard to any situation that could affect the validity of the mechanism or the security of access.

5. PRICE

The services under this Agreement are provided free of charge. However, in the future ENAGÁS reserves the right to establish a price for the foregoing services based on duly informed criteria, in which case it shall notify this to SUBJECT at least 30 days prior to coming into force. Within this deadline, SUBJECT must notify its decision to reject the price specified by ENAGÁS. Lack of such notification within the aforementioned deadline shall be understood as acceptance of the price established by ENAGÁS.

6. DURATION

This Agreement shall come into force from the day following the signing of the Document of Accession to the same and shall have an initial term of two years. It may be tacitly extended for successive periods of one year unless one Party notifies the other of its wish to terminate the Agreement two months before the Agreement termination date or the expiry of any of its extended periods.

7. LIABILITY

7.1 Each Party shall answer to the other party for damages caused to the other as a consequence of acts or omissions involving gross negligence or deceit.

7.2 Except in cases of fraud, the Parties shall only liable for damages directly caused by them. Liability for indirect and consequential damages is hereby expressly excluded. This includes, without limitation, business or trading losses (including loss of profits, revenue, contracts, anticipated savings, data, loss of goodwill or unnecessary expenditure incurred), and any other damages that were not reasonably foreseeable by the Parties at the time the SUBJECT had begun to use the services of ENAGÁS.

7.3 The Parties hereby mutually exempt each other from any damage that might occur, irrespective of the cause -including negligence of the Parties- in their respective facilities and/or systems, as well as their personnel and/or properties, except as provided for in subclause 7.1 above.

The Parties shall not be liable for failure to perform or delay in the performance of the obligations assumed under this Agreement or the Declaration of Certification Practices published by ENAGAS, if such lack of performance or delay is the result or consequence of a case of force majeure or unforeseeable circumstances or in general any circumstance over which they cannot have reasonable control and which include: natural disasters, war, state of siege, disturbances of public order, transportation strikes, power failure and/or phone cut-off, computer viruses, deficiencies in telecommunications services, security breaches of the certification system or any damages arising from an event caused by an unpredictable advance in the art.

7.4 ENAGÁS shall not be liable for the acts or omissions which, as a consequence of access under this Agreement, are carried out by SUBJECT, or any of the users designated by this party pursuant to Clause 4.

ENAGAS shall not be liable for damages arising from or related to the failure to perform or defective performance of the obligations of SUBJECT and/or of the subscribing users, or for the incorrect use of the authentication methods and codes, or for any indirect damages that could result from use of the authentication method or the information supplied by ENAGÁS. ENAGÁS shall not be liable for any possible inaccuracies in the identification of users as a consequence of information furnished by SUBJECT or the users.

ENAGÁS shall not be liable for the content of those documents signed or encrypted digitally.

ENAGÁS shall not be liable for the proper performance with applications that are not approved, and for any damages caused by the inability to use such applications.

ENAGÁS shall not be liable for deterioration or malfunctions of the computer equipment or the data on grounds not directly attributable to the use of authentication methods, and provided SUBJECT or the subscribing user do not act with the appropriate diligence.

Irrespective of the grounds on which ENAGÁS may be charged with liability under this Agreement, the claim for damages cannot exceed, except in the case of fraud, the figure of € [60,000].

8. **ASSIGNMENT**

8.1 ENAGÁS may perform a one-off transfer of its position in this Agreement through any act in the law to any other company that is part of ENAGÁS Group, and must notify this to SUBJECT.

8.2 SUBJECT cannot assign or transfer the rights and obligations stemming from this Agreement in full or in part without prior written consent from ENAGÁS. Breach of this obligation by the SUBJECT shall be sufficient cause for the termination of this Agreement.

8.3 Under all circumstances, the Assignee shall fully assume all rights and obligations arising under this Agreement, whether before or after the time the assignment is effective.

9. TERMINATION OF THE AGREEMENT

This Agreement may be terminated on any of the following grounds:

- At the discretion of the Party not in breach, whenever there is serious breach by the other Party of any of its main obligations under this Agreement. To this end, the Party that considers there to be an event of breach shall notify the other Party of said breach, duly compelling them to rectify said breach. Failure to rectify the breach within 10 calendar days following the aforementioned notification shall entitle the Party not in breach to terminate this Agreement.

- Through termination of the initial term or any of the extensions thereto, in accordance with the terms laid down in Clause 6.

- Through the will of either Party, duly providing the other Party with at least two months’ notice in a manner requiring acknowledgement of receipt.

- At the discretion of both Parties, when an event of force majeure may hinder or prevent compliance with the Agreement for more than one (1) month.

- Through breach of the obligations set out in foregoing Clause 8.2.

- By mutual agreement of the Parties.

10. COMMUNICATIONS

All communications between the Parties concerning this Agreement shall be made in accordance with the provisions set out in the Document of Accession to the same.

11. APPLICABLE LAW AND JURISDICTION

11.1 This Agreement shall be governed by common Spanish legislation.

11.2 The Parties hereby undertake to comply with this Agreement in good faith, using negotiations and amicable agreements to resolve any differences that may arise between them with regard to the application, development, compliance, interpretation and performance of the same.

11.3 The Parties expressly submit to the jurisdiction and terms of reference of the Courts of Madrid for ruling on any dispute or litigation concerning the Agreement, in particular with regard to its interpretation, performance or non-performance, whether before or after its expiry, and which, in the opinion of one of the Parties, they are unable to resolve through mutual agreement.

11.4 The submission of conflicts between the Parties to the foregoing judicial bodies does not entitle either Party to suspend compliance with their obligations under this Agreement.

12. PERSONAL DATA PROTECTION

12.1 Purpose

ENAGÁS, as a consequence of the activity it provides to the DATA SUBJECT, accesses personal data that is the responsibility of the DATA SUBJECT. For these purposes, the DATA SUBJECT will be considered the data controller (hereinafter DATA CONTROLLER) and ENAGÁS will be considered the data processor (hereinafter, DATA PROCESSOR) in accordance with the provisions of articles 28 and 29 of the (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, GDPR).

12.2 Description of the Processing

The data affected by this Agreement will be used for the sole purpose of identifying and authenticating the persons who access the systems that are the subject of the Agreement on behalf of the DATA CONTROLLER.

12.3 Information affected

For the performance of the services arising from compliance with the purpose of the assignment, the DATA CONTROLLER places the following information at the disposal of the DATA PROCESSOR.

- Name and Surname(s).
- National Identity Document
- Work email address.
- Work mobile telephone number.

12.4 Obligations of the DATA CONTROLLER

The DATA CONTROLLER undertakes to:

1. Furnish the DATA PROCESSOR with the data covered by the processing specified in this Agreement.

2. Carry out an assessment of the risks involved in the processing and, when appropriate, an impact assessment of the data processing that the data processor must carry out.

3. Notify the competent Supervisory Authority of any security breaches in accordance with article 55 of the GDPR without undue delay, and in any case within the 72-hour deadline from becoming aware of these. If the supervisory authority is not notified within 72 hours, the reasons for the delay must be appended.

4. Notify the data subjects of any data security breaches as expeditiously as possible, when it is likely that the violation poses a high risk to the rights and freedoms of natural persons.

5. Ensure, prior to and throughout the processing, compliance with the GDPR by the DATA PROCESSOR.

6. The DATA CONTROLLER must facilitate the right to be informed at the time when the data is collected. The DATA PROCESSOR does not collect personal data for and on behalf of the DATA CONTROLLER. The data accessed by the DATA PROCESSOR pursuant to this Agreement must be obtained and processed pursuant to prevailing regulations governing personal data protection.

12.5 Obligations of the DATA PROCESSOR

Taking into account the nature, scope, context and purposes of the processing, the DATA PROCESSOR will apply the technical and organisational measures defined in this Agreement to guarantee a level of security appropriate to the involved risk, complying with the following obligations:

1. Principle of data minimisation

Access the personal data that is the responsibility of the DATA CONTROLLER only when it is essential for the proper performance of the services for which the party has been contracted.

2. Restriction of purpose

Not to assign, apply or use the personal data that are the responsibility of the DATA CONTROLLER for a purpose other than that specified in this Agreement, or in any other way that implies a breach of the instructions of the DATA CONTROLLER.

3. Responsibility

To assume the status of DATA CONTROLLER if data are used for a purpose other than compliance with the purpose of the Agreement, disclosed or used in breach of the stipulations of the Agreement or the obligations of prevailing regulations, duly answering for any infringements incurred.

4. Non-disclosure of data

Not to permit access to personal data provided by the DATA CONTROLLER to any employee under their charge that does not need to access these data to provide the services contracted.

Not to reveal, transfer, assign or communicate in any other way the personal data that are the responsibility of the DATA CONTROLLER, either verbally or in writing, by electronic means, hard copy or through IT access, not even for safeguarding purposes, to any third party, unless there is prior authorisation or instruction from the DATA CONTROLLER.

5. Records of Processing Activities

If required to keep Records of Processing Activities under article 30 of the GDPR, the DATA PROCESSOR will keep a record of all categories of processing activities carried out on behalf of the DATA CONTROLLER, which contains the information required under article 30.2 of the GDPR.

6. Training

Guarantee the necessary training in terms of protection of personal data of the persons authorised to process personal data.

7. Enquiries to the Supervisory Authority

Support the DATA CONTROLLER in making preliminary enquiries to the Supervisory Authority, when applicable.

8. Supervision

Provide the DATA CONTROLLER with all of the information required to demonstrate compliance with its obligations, as well as to conduct the audits or inspections undertaken by the DATA CONTROLLER or another auditor authorised by this party.

9. Security measures

Adopt and apply the following security measures, in accordance with the assessment of the risk carried out and, where appropriate, the Impact Assessment, pursuant to article 32 of the GDPR (that guarantees the security of the personal data of the DATA CONTROLLER), to avoid their alteration, loss, processing or unauthorised access, in light of the state-of-the-art, the nature of the data stored and the risks to which they are exposed, whether as a consequence of human action or physical or natural means.

The security measures applicable to data processing are for the following purposes:

a) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

c) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, and;

d) the pseudonymisation and encryption of personal data, where necessary.

To this end, the following measures are introduced:

a) Control of access to the SL-ATR systems through the establishment of identification and authentication measures.