General Contract Conditions - Digital Certification Services - Holder

General Provisions

These General Conditions of the Contract for the provision of Digital Certification Services (hereinafter, “General Conditions”), govern the procedures and terms according to which the Company, Actalis S.p.A., (VAT Reg. 03358520967) with headquarters at Via San Clemente 53, 24036 Ponte San Pietro (BG), also by way of the activities undertaken by the CDRL, supplies to the Holder the Service, based on the procedures indicated in these general conditions and in the operating manual prepared by Actalis

Index of the Articles

General Provisions 1
1. Definitions 1
2. Purpose of the Contract 3
3. Structure of the Contract 3
4. Execution of the Contract 3
5. Fees, payment procedures and billing 3
6. Request for Registration and issue of the Certificate and activation 4
7. Duration of the Contract and Validity of the Certificate 4
8. Customer/Holder’s Obligations 4
9. The Certifier’s obligations and limitation of Liability 6
10. Hardware or Software for Certificate operation 6
11. Support 7
12. Reference to the Manual 7
13. Comms 7
14. Modification to the services and changes to the Conditions of the Offer 7
15. Rescission of the contract, express termination clause 7
16. Withdrawal 7
17. Revocation and suspension of the Certificate 7
18. Disclosures pursuant to art. 5, 52, 53, 64 et seq. of Legislative Decree 206/2005 and pursuant to art. 7 of the Legislative Decree 70/2003 8
19. Final provisions and communications 9
20. Applicable Law 9
21. Competent Court 9
22. Processing of personal data 9
23. Appointment of the Data Processor 10

1. Definitions

For the purposes of these General Conditions, the following definitions shall apply:

Agency for Digital Italy: a non-profit public entity, with authority over the sector of information and communication technologies within the area of public administration;
Actalis: Actalis S.p.A.: an Aruba Group company, registered in the public directories of Certifiers and Trust Service Providers established, kept and updated by the Agency for Digital Italy (hereinafter, "AgID"), which issues legally valid Digital Signature Certificates and eIDAS Seals and delivers the qualified Temporary Electronic Validation Service as a Qualified Trust Service Provider pursuant to Regulation (EU) No. 910/2014 and the implementation legislation (hereinafter, "Actalis" or "Certifier"), to Legislative Decree no. 82/2005 and Prime Ministerial Decree of 22/02/2013, as subsequently amended and supplemented (hereinafter, "Actalis" or "Certifier");
CAD: Legislative Decree No. 82 of 7 March 2005, as amended and supplemented;

Local Registration Centre (CDRL): the party, which pursuant to the independent contract stipulated with Actalis, is authorized by the latter to perform activities for the purpose of issuing digital certification services;
Authentication certificate: The Certificate consisting of the electronic certification guaranteeing the authenticity of the information required for the online identification of the holder of the CNS issued by Actalis as authorized by the Issuing Body as set forth in Presidential Decree no.117 of 2 March 2004 and in the CNS Operating Manual, and which grants access to the information systems held by the Government Authorities;
Signature certificate: The Certificate that connects the data used to verify the Digital Signature to the holder and to confirm the identity thereof, issued by the Certifier, ACTALIS S.p.A., as set forth in art. 3, paragraph 1, no. 15 of the Regulation, in the CAD, in the technical regulations referred to therein and in the Operating Manual.
Certificate: the definition used in the Contract to refer without distinction to the Signature Certificate and/or the Authentication Certificate and/or the eIDAS Seal when it is not necessary to specify the certificate concerned;
Private key: the part of the pair of asymmetric keys designed to be known exclusively to the party that is the holder thereof, by means of which the latter attaches the Digital Signature to an electronic document or decrypts an electronic document that has been encrypted using the corresponding Public Key;
Public Key: the part of the pair of asymmetric keys designed to be made public, by way of which one verifies the Digital Signature attached to the electronic document by the holder of the asymmetric keys or one encrypts electronic documents to be sent to the holder of said keys;
Customer: the party identified in the Digital Signature Application Form, who, in the capacity of Holder, applies for the provision of the Digital Signature Device referred to in this Contract (hereinafter, User or Holder);
CNS: acronym for National Service Card, as defined in the CAD, i.e. the instrument used to gain access to the services provided online by the public authorities for which electronic identification is required;
Certifier Contact: the personnel appointed by the Certifier to provide assistance to the Users on the use of the Digital Signature Device by way of the contact details indicated on the website https://www.actalis.com/it/contatti.aspx ;
Contract: document made up of the Digital Signature Application Form, of these General Contract Conditions and of the Operating Manual;
Digital Signature Device: the Digital Signature solution, with or without CNS, described in detail in the Manual applicable to the Certificate requested and distributed by Actalis to the Customer, as stated by him/her in the Order Form.
Device for the creation of a qualified electronic signature: the device for the creation of an electronic signature satisfying the requirements in the Regulation.
Issuing Body: The Public body that, having authorisation to issue the Authentication Certificate for the purpose of executing the contract, instructs Aruba to issue and manage it electronically;
Automatic Signature: specific IT-based digital signature process undertaken following authorization by the signatory holding exclusive control of the respective signature keys, in the absence of immediate, on- going protection by the latter;
"One shot" digital signature: a particular type of remote Digital Signature based on a signature certificate that may only be used for signing documents originating from specific so-called "one shot" electronic processes, provided on the website www.pec.it and in accordance with the terms and limitations set out in the Manual and in the Contract.
CNS digital signature: a type of electronic signature also containing the Authentication Certificate;
Remote digital signature: particular type of digital signature, generated on HSM under the full control of Actalis, which guarantees to the Customer exclusive control of the private keys; at the Customer's request, this signature can also be supplied with the "Verified Procedure" option as set forth in art. 19 of the Prime Ministerial Decree of 22 February 2013;
"Remote Automatic Identity Proofing (RAIP)" application: the software application made available by Aruba which uses liveness and biometric techniques based on artificial intelligence (AI) for the purpose of remotely identifying the person requesting the eIDAS Certificate and eIDAS Seal.
Digital signature: a particular type of advanced electronic signature based on a qualified certificate and on a system of cryptographic keys, one public and one private, related to one another, which enables the Customer, via the private key, and the recipient, via the public key, respectively, to reveal and verify the source and integrity of an electronic document or of a set of electronic documents;
HSM: a set of hardware and software that creates secure devices for the generation of signatures capable of securely dealing with one or several copies of cryptographic keys;
Privacy Policy Actalis: public document available at https://actalis.com/documents/tc-files/en/en-privacy-policy-actalis.aspx describing processing of the Customer's personal data.
"National Service Card – CNS" Operating Manual: the manual published and made public in accordance with the law, containing details of the procedures for issuing the Authentication Certificate (when, together with the "Certification Services" Operating Manual, the Manual or also the "Manuals") available for download at the link https://www.actalis.it/area-download.aspx);
Qualified Certificates Operating Manual: the manual published and made public in accordance with the law, containing details of the processes for issuing the Signature Certificate (when, together with the "National Service Card – CNS" Operating Manual, the Manual or also the "Manuals") available for download at the link https://www.actalis.it/area-download.aspx).
Service Practice Statement (SPS) Manual "Remote Automatic Identity Proofing – RAIP & S-RAIP": the legally published and public manual containing the description of remote identification procedures carried out by means of the artificial intelligence software application called "Remote Automatic identity proofing" for the purpose of issuing the eIDAS Certificate and eIDAS Seal. The Manual at issue is available at: http://www.pec.it/termini-condizioni.aspx. The Manual at issue describes in detail: i) the Remote Automatic Identity Proofing – RAIP, i.e. a fully automated remote identification process; and ii) the Supervised Remote Automatic Identity Proofing – S-RAIP, i.e. a remote identification process performed using an optional and subject to a fee variant with human supervision.
Manual(s): the definition used in this Contract to refer interchangeably to the "Certification Services" Operating Manual, the "National Service Card – CNS" Operating Manual, when it is not necessary to specify the Manual concerned;
Verified mode: The terms that subject the use of the Remote Signature to verification of its validity by Actalis, namely that the corresponding certificate has not expired, been suspended or revoked when the signature is generated;

Renewal Form: electronic form available from the member's area of the website using the access credentials, which, when fully completed by the Holder and sent by it to the Certifier, constituting a contractual proposal, formalises the request for renewal of the Remote Signature Service or the Digital Signature Service
Order Form: the form wich, when fully completed online By the Customer and sent by the latter to the Certifier, constituting a contract proposal, formalises the Application to renew the Digital Signature Device for the Digital Signature;
Digital Signature Application Form: the form for applying for the Certificate completed by the Customer in which the latter indicates the information necessary for respective identification;
Legal entity: the collective which, in the case of a request for eIDAS Seals, is the Holder of the seal issued;
PKI Disclosure Statement (PDS): the document, which together with the Qualified Certificates Operating Manual, with this Contract and with the applicable regulations, governs the service of issuing signature certificates and eIDAS seals;
Regulation: 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", the technical regulations referred to therein, the European Commission's implementing acts thereof and any subsequent amendments and additions.
Remote in-person identification: process whereby the Certification Authority, as set out in the Manual, undertakes the positive identification of the Customer in accordance with art. 32, paragraph 3, letter a, of Legislative Decree 82/2005, as required for the issuing of the Certificates.
eIDAS Seal: this is the Certificate in the form of qualified electronic seal as per art. 3, paragraph 1, no. 15 of the Regulation and governed by the Qualified Certificates Operating Manual.
Terms and Conditions for the Use of the "Remote Automatic Identity Proofing" Application - RAIP & S-RAIP: the terms and conditions governing the Customer's use of the "Remote Automatic Identity Proofing" application.
T.U.: Consolidated act on the legislative and regulatory provisions on administrative documentation approved by way of Presidential Decree 445/2000.
Interested Third Party: party which, in the event of the issue of Certificates to sign on the basis of a role or positions held on behalf of third-party organizations that provide for the granting of powers, by third parties, to the party applying for the Certificate, together with the Holder, with a direct interest in the management of the Certificate, is authorized to revoke and/or suspend the Certificate.
Holder: the Party in whose name the Certificate(s) is/are issued on the basis of the Application Form.

Any definitions not specifically referred to herein shall retain the meaning attributed in the Manual applicable to the individual Certificate.

2. Purpose of the Contract

2.1 These General Conditions of the Contract for the provision of Digital Certification Services (hereinafter, "General Conditions"), govern the procedures and terms according to which the Company, Actalis S.p.A., (VAT Reg. 01879020517) with headquarters at Via San Clemente 53, 24036 Ponte San Pietro (BG), by way of the activities undertaken by the CDRL/IR, supplies to the Customer the Digital Signature Device, based on the procedures indicated in these general conditions and in the operating manual prepared by Actalis.
2.2 The Digital Signature Device is offered and marketed according to the technical characteristics and financial conditions specific to the individual commercial offer pre-selected by the Customer from those made available thereto, and as is in legal terms and in actual fact on the application date, which the Customer, accepting the following General Conditions, explicitly declares to know and accept.
Through the supply of the Digital Signature Device, the Customer is provided with tools implementing an electronic process, through which to request, issue, use, suspend, revoke and renew a Certificate.
2.3 The offer of said services is for an open-ended time period, subject to the right of Actalis to suspend or revoke it at any time; in such case, the contracts entered into before said suspension and/or revocation shall be honoured according to the agreed conditions.

3. Structure of the Contract

3.1 The Digital Signature Device Supply Contract is made up of the following documents:
a) Application Form (hereinafter, "Form"), which includes a contractual proposal put forward by the Customer;
b) General Contract Conditions - Digital Certification Services, drafted and prepared in observance and in compliance with the provisions contained in Legislative Decree 206/2005 and in Law 40/2007, have a general scope and may undergo changes made necessary by subsequent legal provisions and/or regulations;
c) Manual applicable to the CERTIFICATE TYPE requested, in the version published at the time of the Digital Signature Device supply application, which the Customer is expressly required to consult before sending the Digital Signature Device order. The publications of the Manual are available in electronic format on the Certifier's corporate website, at the link (https://www.actalis.it/area-download.aspx), in electronic and paper format from the Agency for Digital Italy (http://www.agid.gov.it/), and in paper format from any Local registration Centre;
d) PKI Disclosure Statement (PDS) containing provisions for the issue and rules of Signature Certificates and eIDAS Seals.
3.2 The Customer acknowledges and accepts that the sending of the Form constitutes acceptance of these General Conditions and of the Manual applicable to the requested Certificate referenced by the General Conditions, which shall be fully effective and binding for the Customer, regardless of the intervening execution of the Contract and subsequent supply of the Digital Signature Device.

4. Execution of the Contract

The contract is considered executed upon issue of the requested Certificate.

5. Fees, payment procedures and billing

5.1 Subject to that set forth in the Contract and unless otherwise agreed by the Parties:
a) The Customer is required to pay the fee for the Digital Signature Device indicated in the Offer, based on the rates in effect at the time of the order, which vary according to the type of Digital Signature Device chosen;
b) Upon expiration, if the Certificate is renewed by the Customer, the latter shall be required to pay the fee indicated in the list in effect published at the time of the renewal.
5.2 The VAT due shall be applied to any invoiced amounts and, together with any other tax charge resulting from performance of the contract, shall be borne by the Customer. In any case, the Customer hereby expressly declares to release the Certifier from all and any liability resulting from any transactions or payments made. The Customer may not assert rights or raise objections of any kind unless he/she has first made the payments set forth in the contract correctly or if they have not been duly made and confirmed.
5.3 It is hereby understood that any further agreements arising between the Customer and the CDRL/IR shall only be effective as to relations between them.

6. Request for Registration and issue of the Certificate and activation

6.1 The Customer must request the Digital Signature Device according to the procedures indicated in the Manual applicable to the Certificate requested, by completing the specific Form.
6.2 Specifically, the Customer agrees to communicate to the Certifier:
a) details, documents, correct and truthful information, specifying which of the pieces of information provided he/she wishes to exclude from the certificate;
b) the existence of any restrictions on the use of the pair of certification keys (by way of example, powers of representation, restrictions on powers, etc.), substantiated by suitable documentation;
c) in a timely manner, any amendment to the information or details provided.
In addition, the Customer is required to generate the pair of keys for secure signing, in accordance with the procedures set out in the Manual.
6.3 Actalis shall proceed with issuing the Certificate, strictly according to the chronological order of the requests received, if complete and correct as to their content. The Digital Signature Device, with or without the Authentication Certificate, as requested by the Customer, shall only be issued in the event of a positive outcome of the checks required for this purpose; in the event that the Certificate is not issued, Actalis shall notify the Customer of the reasons for said certificate not being issued.
6.4 Actalis shall notify the Customer/Holder of issue of the Certificate. It is hereby understood that the activation of the Certificate, except for those to be used with the remote Digital Signature Service, must be undertaken directly by the Holder through the appropriate procedure in compliance with the following timing:

- within 90 calendar days of receiving the verification link, the Certificate Holder must correctly complete the verification procedure. In such cases, the Certificate Holder is not permitted to use verification methods other than those expressly provided for in the CPS (Certificate Policy Standard) Manual in effect at the time;
- once the verification has been successfully completed, the Certificate Holder must activate the Certificate within the following 90 calendar days. Activation constitutes confirmation of the accuracy of the data contained in the certificate or seal and acceptance of such data.

It is understood that if even one of the two deadlines mentioned above is not met, or if the validity requirements of the identification procedure described above are not met, the Certificate will no longer be usable. In such a case, the Holder must, if necessary, purchase a new digital signature device without being entitled to make any claim against Actalis, including for a refund, for the Certificate that has become unusable.
6.5. With specific reference to the eIDAS certificate, if the Customer purchases the certificate for third parties authorized by the Customer, as Holders of the Certificate, the Customer must inform the third parties of the conditions and obligations that apply to the Service and communicate to them the application for issuing the Certificate and provide them with a hard copy of this Contract, of the applicable Manual and of the issue application.
6.6 The Customer/Holder acknowledges and accepts that, in order to perform the services governed by this Contract, certain data that he/she provided when requesting the issuing of the Certificate shall be published, as indicated in the applicable Operating Manual. The Customer accepts that said data, in the event of the termination of the certification activity, may be communicated to an alternative certifier or Trust Service Provider or to another identified party in compliance with the requirements of the applicable legislation.
6.7 The data provided in order to activate the service shall be stored for the period of time established by applicable legislati on, as described in the Manual applicable to the pre-selected service.
6.8 In order to request an eIDAS Seal the Customer must present the relevant documentation as set out in the CPS Manual pertaining to the legal entity that will be the Holder of the seal, as well as documentary proof of the Customer's powers of representation with respect to said legal entity.
6.9 The Customer/Holder expressly acknowledges and accepts that in cases of remote identification through the use of the artificial intelligence software application called “Remote Automatic Identity Proofing”, the contractual terms and conditions expressly set out in the SPS Manual “Remote Automatic Identity Proofing – RAIP & S-RAIP” (section 54 “General Terms”) shall apply.

7. Duration of the Contract and Validity of the Certificate

7.1 The term of the contract is the same as the duration of the Certificate indicated therein, in the "validity" section.
7.2 As the expiration date draws near, as a mere courtesy and therefore without thereby assuming any obligation vis-à-vis the Customer/Holder, the Certifier shall have the right to send notice of the imminent Certification expiration to the email address indicated during the order phase.
7.3 It is possible to request renewal of the Certificate before it expires, it is possible to request renewal of the Digital Signature Certificate in the manner stated by the Certifier, by sending the specific Order Form and paying the respective amount due, according to the rates

and conditions in force at the time of renewal for the option chosen from those made available. Renewal of the certificate shall lead to extension of the contract until the expiration date of the renewed certificate or revocation thereof. The Customer acknowledges and accepts that by activating the renewed Certificate, the preceding certificate shall no longer be valid and usable. Under no circumstance may an expired or revoked Certificate be renewed.
7.4 Without prejudice to the foregoing, when requesting or renewing the Signature Certificate and accepting these General Conditions, the Customer shall be entitled to activate the tacit renewal mode for the Remote Digital Signature Certificate. If the Customer exercises this option, on the expiry date of the Remote Digital Signature Certificate the same shall be automatically renewed according to the procedure described in the Operating Manual. The Customer may at any time deactivate the tacit renewal mode of the remote digital

signature Certificate in accordance with the terms and procedures established by the Certification Authority.
The Customer acknowledges and agrees that, in the event that the hardware device (digital signature device) on which the Certificate is stored is lost or the security certification required by applicable regulations expires, the device will no longer be usable and, consequently, the digital signature certificate will be revoked by Actalis in accordance with the procedures set forth in the Operating Manual. 7.6 If the QSCD compliance certification associated with the digital signature device (smart card or equivalent device) expires or is revoked early, and at the same time the CNS certificate installed on the same device remains valid, the Customer may be entitled to activate an external remote signature service free of charge.
This remote signature service will have a duration equal to the remaining validity period of the digital signature certificate not used by the Customer due to early revocation.
It is understood that the use of the external remote signature service is subject to the continued validity of the CNS certificate installed on the device.
The external remote signature service may be used exclusively through the applications made available by the Aruba PEC Certification Authority. In order to activate and use the service, the Customer must have an Internet connection and the Aruba Sign application software provided free of charge by the Aruba PEC Certification Authority.

8. Customer/Holder's Obligations

8.1 The Customer/Holder's obligations are those indicated in the Manual applicable to the requested Certificate, in the documents and legal provisions referenced therein and in these General Conditions.
8.2 The Customer/Holder, aware that:
a) the Signature Certificate and the eIDAS Seal allow records and documents relating to the Holder to be signed for all legal purposes within the context of the European Union;
b) the Authentication Certificate is an online identification tool that allows for the use of government services,
c) the Signature Certificate and the eIDAs Seal must be used in conjunction with the data held on a device for the creation of a qualified electronic signature, as defined in art. 3, paragraph 1, no. 23 of the Regulation;
d) the certificates or seals issued on the basis of the provisions of this Section II must be used for the purpose described in the "KeyUsage" field therein, and any other use may result in the electronically signed documents being invalid and/or the services provided by third parties being inaccessible. Comprehensive information on the use of each certificate/seal can be found in the relevant Manual;
is required to take the utmost care in the use, storage and protection of the private key, the Digital Signature Device and the activation code (PIN) associated therewith, as well as any additional codes provided by the Supplier for the use of the Service. In particular, the Customer/Holder is required to adopt all the appropriate measures to prevent the harming of others from use of the asymmetric keys system or Digital Signature Device. In addition, the Customer/Holder is required to protect the secrecy of the Private Key by not communicating or disclosing to third parties the Personal Identification Number (PIN) for activation thereof, by entering it according to procedures that do not allow it to be discovered by other parties and by keeping it in a safe place and separately from where the device containing the key is safeguarded. The Private Key, for which the Signature Certificate has been issued, is strictly personal and may not for any reason be assigned or provided for use to third parties. The Customer/Holder acknowledges being exclusively responsible for the protection of his/her own Private Key (contained in the signature device/Smart Card) from damage, losses, disclosures, alterations or unauthorized uses. The Customer/Holder agrees to use the Digital Signature Device in compliance with the provisions in the Contract and on the company website, in accordance with the law, current legislation, ethics and public order. To illustrate, though not exhaustively, the Customer/Holder agrees:
a) to abstain from committing any breach of the systems or of network security that may give rise to civil and/or criminal liability;
b) not to use the Digital Signature Device in such a way as to cause harm to him or herself or to third parties;
c) to use the Digital Signature Device only for the uses permitted by law with a prohibition including, but not limited to, sending, publishing and/or sharing material:
c.1) that breaches or infringes intellectual property rights, trade secrets, trademarks, patents or other legal or customary rights;
c.2) featuring contents in breach of ethics and public order for the purpose of disturbing public and/or private peace, causing offence or direct or indirect harm to anyone;
c.3) featuring child pornography, pornography or obscene content or in any case content in breach of public morals;
c.4) considered to violate or to attempt to violate the confidentiality of private messages or intended to harm the integrity of the resources of others or cause direct or indirect damage to anyone (counterfeit software, cracks, key generators, serials, viruses, worms, Trojan horses or other harmful components);
c.5) capable of engaging in Spamming or equivalent activity;
d) to ensure that the personal data communicated to the Certifier for the full performance of the contract is correct, up-to-date and accurate and makes it possible to identify his or her true identity. The Customer acknowledges and agrees that, if he or she provides

false, non-current or incomplete data, the Certifier reserves the right to suspend/disable the Digital Signature Device and/or rescind the contract, thereby withholding the sums paid by the Customer and reserving the right to request compensation for further damages; it is hereby understood that the Customer may not submit to the Certifier any request for reimbursement, indemnity and/or compensation for damage for the time during which he or she did not make use of the Digital Signature Device;
e) to keep harmless and release the Certifier from any liability in the event of complaints, lawsuits, administrative or judicial actions, losses or damages (including legal costs and fees) brought about by the illegal use of the services by the Customer him or herself;
f) to use the Signature Certificate and the eIDAS Seal in conjunction with the data held on a device for the creation of a qualified electronic signature, as set forth in art. 3, paragraph 1, no. 23 of the Regulation;
g) to use the Certificates in compliance with the use described in the "KeyUsage" field existing therein, acknowledging that any other use may result in the electronically signed acts and documents being invalid and/or the services provided by third parties being inaccessible.
Comprehensive information on the use of each certificate/seal can be found in the relevant Manual.

8.3 In the event of Automatic Signature, the service makes it possible to use, through specific application interfaces, the Automatic Signature infrastructure with Certificates issued by the Certifier.
Aware that use of an Automatic Signature for which the respective Certificate has been issued involves the possibility of signing instruments and documents pertinent in all respects to the law within the scope of the European Union, solely attributable to the party in whose name it has been issued, the Customer/Holder acknowledges:
a) that he/she is solely responsible for use of the private key, the signature device and the activation code (PIN) associated therewith;
b) his/her obligation to take all the appropriate measures to prevent the harming of others from use of the asymmetric keys system or Automatic Signature.

8.4 The Customer/Holder is also liable for any damage suffered/to be suffered by the Certifier and/or by third parties in the event of a delay on the Customer's part in triggering the processes set out in the Manual applicable to the Certificate for the revocation and/or suspension of the Certificate.

8.5 Should the Customer, on identification, also by the use of false personal documents, have concealed his/her true identity, falsely declared to be another party, falsely declared the existence of powers of representation, indicated untruthful data on the Holder or, in any event, acted in such a way as to compromise the identification process and the respective findings indicated in the certificate, he/she acknowledges and accepts that he/she shall be held civilly and criminally liable for the false declarations and/or the use of false documentation and shall also be considered solely liable for all damages suffered and to be suffered by the Certifier and/or by third parties due to the inaccuracy and/or falsehood of the information contained in the certificate, assuming henceforth the obligation to hold harmless and release the Certifier and third parties from any claim, action and/or request for indemnity or compensation for damage that may be brought against them by anyone.

8.6 In the event of breach of even just one of the aforementioned obligations/commitments, the Certifier shall have the right to intervene in the manners and forms considered appropriate to eliminate, if possible, the breach and its effects, and to suspend/disable immediately and without any notice the Digital Signature Device and/or to revoke the issued Certificates, thereby also reserving the right to rescind the contract pursuant to art. 15 below. The sums paid by the Customer shall be withheld for compensation, without prejudice in any case to compensation for further damage. The Customer acknowledges and agrees that he or she shall have nothing to claim from the Certifier for reimbursement, indemnity or compensation for damage due to measures that the latter has considered appropriate to take. In any case, the Customer hereby takes on full responsibility regarding the above violations and agrees to hold harmless and release the Certifier from all and any direct or indirect liability, expense, harm or damage arising from claims or actions by third parties under which the Certifier is held liable to third parties due to an act attributable to the Customer, including, but not limited to, liabilities and damage resulting from any erroneous or out- of-date information or details issued to the Certifier, from incorrect implementation of the procedures described in the Operating Manual.

8.7 The Customer acknowledges and accepts that, during the contract term, the Certifier reserves the right to request therefrom, at any time, the provision of suitable documentary evidence of his/her identity, his/her address or residence and of the accuracy of the details communicated at the time of the application to issue the Certificate or in any case during the term of the contract.

8.8 Before signing the Application Form, the Customer agrees to obtain information and to inform the Holder if not the same person, about the legislative, technical and financial conditions, usage procedures, and the obligations and duties that govern the certification service requested by the same.

8.9 The Customer guarantees, with reference to third-party data handled by him or her at the order stage and/or during use of the Service, that said parties have been provided in advance with the information referred to in Article 13 of EU Regulation 2016/679 and that they have an appropriate legal basis for the processing. In any event, it is understood that, in relation to such data, the Customer shall act as Data Controller, assuming all the obligations and responsibilities associated with this role and holding Actalis harmless against any dispute, claim or other demand that may come from third parties with reference to such processing circumstances.

8.10 With reference to the use of the "Remote Automatic identity proofing" application, the Customer/Holder is obliged to use this application made available by Aruba in compliance with the laws, the regulations in force, the General Conditions of Use of the Application, the SPS Manual "Remote Automatic Identity Proofing"– RAIP & S-RAIP" as well as these General Conditions for the supply of the Services, the specific limits and methods of use applicable to them and made known and updated also through the website www.aruba.it / www.pec.it.

8.11 The Customer/Certificate Holder agrees to use the private key associated with the certificate exclusively for the purposes and objectives for which the certificate was issued, in compliance with the provisions contained in these General Terms and Conditions, in the Manual applicable to the requested Certificate, and with any restrictions on use expressly indicated in the certificate itself. The Customer/Certificate Holder undertakes to refrain from any use of the aforementioned private key for purposes other than, incompatible with, or exceeding those permitted, and acknowledges that any use made in violation of this obligation shall be under the Customer's sole responsibility.

9. The Certifier's obligations and limitation of Liability

9.1 Actalis' obligations are those indicated in the Manual applicable to the Certificate and in the documents referenced therein. Actalis hereby assumes no obligations other than those set forth in these General Conditions, in the Manual and in the relevant laws currently in force.
9.2 Actalis does not provide any guarantee in the event of improper and/or incorrect use of the Digital Signature Device with respect to that established by current provisions and by the applicable Manual. Aruba Pec does not provide any guarantee on the correct operation and safety of hardware and software used by the Customer, on the regular and on- going operation of national and/or international electricity and telephone lines, on the validity and importance, even on a trial basis, of the Certificate or of any message, instrument or document associated therewith or produced through the keys to which the Certificate refers with respect to parties subject to legislations different from that governing the effectiveness of the Certificate on respective secrecy and/or integrity (in the sense that any breaches thereof, as a rule, may be detected by the Customer or the intended recipient through the specific verification procedure).
9.3 The Customer declares to have read and accepted the limitations of liability as per the applicable Manual. Except in cases of willful malice or serious negligence, Actalis shall not be liable for any damage with respect to the Customer/Holder and/or in any case with respect to third parties. Actalis shall not be liable for any damage and/or delays due to the malfunctioning or failure of the IT system. In any case, Actalis shall not be liable for damage caused to the Customer and/or third parties, once the expiration deadline of 10 (ten) days has lapsed from the harmful event or from the discovery thereof communicated as indicated in the applicable Manual.
9.4 Under no circumstances may Actalis be held liable for any direct or indirect damage suffered by anyone, including the Customer/Holder:

a) caused by improper use of the digital Signature Device or non compliance with the rules and obligations described in these contractual conditions, in the applicable Actalis Manual and on the website https://www.actalis.it/area-download.aspx ;
b) resulting from impossibility of performance, malfunctioning of networks or of technical equipment, force majeure, accidental events or catastrophic events (including but not limited to: fires, explosions, etc.);
c) of any nature and extent suffered by the Customer and/or by third parties caused by tampering or interference with the Digital Signature Device or devices by the Customer and/or by third parties not authorized by the Certifier.

9.5 As far as the eIDAS Seal is concerned, the Customer henceforth acknowledges and accepts that the Certifier assumes no obligation to verify, subsequent to the issuing of the eIDAS Seal, continued compliance with the requirements relating to the legal entity that has consented to it being issued.

10. Hardware or Software for Certificate operation

If requested by the Customer, the Certifier, directly or through Registration Operators or Registration Supervisors, shall deliver to the former, following payment of the respective cost, a signature device (hardware-Smart Card and/or reader) capable of storing and reading its Private Key and of generating the digital signatures.

11. Support

The customer support service is provided in accordance with the procedures set forth in the operating manual and as stated on the website at https://www.actalis.it/area-download.aspx , which is referenced in full.

12. Reference to the Manual

For anything not expressly stated in the above articles, refer to the provisions of the Manual relating to the requested Certificate prepared by Actalis and on the website at www.pec.it, which is an essential and integral part of this contract.

13. Comms.

13.1 Any written communication must be sent by the Customer to the Certifier's contact details indicated in these Conditions**.**
13.2 If in the Form the Customer has indicated an e-mail address, it shall be considered an e-mail address pursuant to art. 14, paragraph 1 of the T.U., and all communications shall be validly sent to the Customer using said address. In the event of failure to indicate an e-mail address, communications shall be sent to the address indicated by the Customer in the Form.

14. Modification to the services and changes to the Conditions of the Offer

14.1 The Holder acknowledges and agrees that the Service covered by the Contract is subject to constantly changing technology; for this reason, Actalis reserves the right to improve the technical characteristics of the Service and the corresponding tools at any time and to amend the Contract conditions at any time, even after its acceptance, without this giving rise to obligations of any kind on the part of the Holder.
14.2 Actalis also reserves the right to amend the Actalis Services User Policy and Actalis Privacy Policy at any time in accordance with legal provisions.
14.3 The Certifier reserves the right to make changes to the provisions of the Manual due to supervening technical, legislative and operational requirements, which shall be effective with respect to the Customer 30 (thirty) days after the communication is published on the corporate website.

15. Rescission of the contract, express termination clause

15.1 This contract shall be rescinded automatically, with consequent suspension/disabling of the Digital Signature Device, in the event

of revocation of the Certificate. Pursuant to and for the purposes of Art. 1456 of the Civil Code, the Certifier has the right to rescind this contract if the Customer/Holder breaches in whole or in part the provisions of arts. 6 and 8 of these General Conditions. In the aforementioned circumstances, rescission shall occur as a matter of law by way of a unilateral declaration by the Certifier, by registered letter with confirmation of receipt, sent to the Customer/Holder, due to which it shall be authorized to revoke the certificate without any notice. In such circumstances, the Customer acknowledges and accepts that sums paid by the former shall be withheld as a penalty, without prejudice in any case to compensation for further damage. The Customer may not submit any request for reimbursement, indemnity and/or compensation for damage for the time period during which he or she did not make use of the certificate. It is hereby understood that the aforementioned legal rescission shall apply without prejudice to other cases of rescission set forth under law.

16. Withdrawal

16.1 The Customer acknowledges and accepts that the service, involving the provision of a customised product, falls under the provisions under art. 55 of Legislative Decree 206/2005 and that, as such, the exercise of the right to withdraw is not permitted. An order may be halted and possibly cancelled if the production relating thereto has not yet been commenced in any way; in such case, the Customer shall be entitled to obtain exclusively the return of the fee paid. In the event of illegitimate cancellation, withdrawal or rescission by the Customer, the sums paid by the former shall be withheld as a penalty, without prejudice in any case to compensation for further damage.
16.2 Notwithstanding the cases of immediate rescission set forth in art. 15, the Certifier shall have the right to withdraw from this contract at any time and without being required to state reasons, by notifying the Customer in writing, with at least 10 (ten) days' notice. In the event of exercise of the right to withdraw, once the aforementioned notice period has lapsed, the Certifier may disable and/or deactivate the Certificate at any time. In this case, the Customer shall be refunded the payment of the Digital Signature Device price corresponding to the unused days until the subsequent, natural expiration of the contract, after deducting the expenses incurred for providing the Digital Signature Device. All and any further reimbursement, compensation or liability of the Certifier or a party involved in supplying the Digital Signature Device, due to non-use by the Customer of the certificate in the remaining period, shall be explicitly excluded.
.

17. Revocation and suspension of the Certificate

17.1 The requirements, procedures and time frames for revocation or suspension of the Certificate are established in this article and in the applicable Manual. The Certifier shall revoke or suspend the Certificate if one of the following circumstances arises:
a) explicit request submitted by the Certificate Holder in writing;
b) request by an "interested third party" (which must be sent in writing pursuant to the provisions of art. 20, Prime Ministerial Decree);
c) request in cases of urgency (in all cases of loss and/or theft of the signature device) submitted by telephone by the Certificate Holder or by an "interested third party", identified through the confidential authentication code issued thereto upon issue of the Certificate;
d) confirmation that the Certificate was not issued according to the procedures indicated in the applicable Manual or in a manner not in compliance with the procedures set forth under current legislation;
e) confirmation of breach of obligations borne by the applicant and/or Certificate Holder;
f) breach of secrecy and/or breaking of the private key;
g) loss of the private key;
h) abuses and falsifications;
i) request originating from the Courts;
l) request originating from the Customer, if not the same as the Holder. With reference to art. 19, paragraph 4, of the Prime Ministerial Decree, the Certifier shall place the Certificate in suspended status (and therefore suspend its validity) in the event that the authenticity of the request may not be ascertained in a timely manner.
17.2 Certificates relating to certification keys may be revoked or suspended in the following cases:
a) loss, removal, theft or compromise of the secret key;
b) malfunction of the signature device;
c) closing of the business.
In such cases, the Holder is required (even in his/her own interest) to notify the Certifier in timely manner thereof. The Certifier shall trigger the procedures for revocation or suspension of the Certificate.
17.3 Revocation/suspension of the certificate may be undertaken by its Holder by way of three different procedures:
a) the sending in writing of an explicit formal request sent to the Certifier, which must contain information on the Holder's and certificate's identification details and the reasons for which revocation/suspension is requested, signed by the certificate Holder.
b) through the service available on the Actalis website on the Digital Signature webserver page explicitly dedicated to suspension highlighted on the main page, using the confidential emergency code sent by Actalis during the Certificate generation phase;
c) by telephone, using the contact details provided at https://www.actalis.com/it/contatti.aspx, entering the confidential emergency code sent by the Certifier when sending the Certificate after it is generated. In any case, said request must be followed by a communication in writing indicating the reasons for which the suspension is requested, signed by the Certificate Holder.
17.4 Revocation/suspension of the Certificate may be undertaken at the unquestionable initiative of the Certifier, regardless of the Holder's intent, if the need is recognised or one of the following circumstances arises:
a) the details indicated in the Certificate undergo change or become out of date;
b) discovery of the compromise or breaking of the private key;
c) breach of the obligations borne by the Certificate Holder, as set forth in current legislation and/or in the Operating Manual;
d) improper use of the Digital Signature Device by its Holder;
e) possible compromise of the certification key or time stamping relating to the Certificate;
f) any justified request originating from the Courts.
The Certifier shall notify the Holder of the reasons for the revocation, as well as the date and time from which the Certificate is no longer valid.
17.5 Revocation/suspension of the certificate may be undertaken at the request of an Interested Third Party. In this case, the suspension

or revocation request must be signed and be received in writing by Actalis. If expressly set forth, the request may also be sent by e-mail, as long as duly signed with the digital certificate of the "interested third party" if the issue thereof was established. In particularly urgent cases, the "interested third party" may request revocation/suspension of the certificate by telephone, using the contact details provided at https://www.actalis.com/it/contatti.aspx by entering the confidential emergency code sent by Actalis when sending the Certificate after it is generated. In any case, said request must be followed by a communication in writing by post or e-mail - signed using a digital signature - indicating the reasons for which the suspension/revocation is requested. As a mere example, the most frequent cases in which an "interested third party" may request suspension or revocation of a certificate are if the third party is an organization (entity, company, association, etc.) that has acquired a series of certificates and has allocated them to its employees, suppliers, customers and/or persons in any way relating thereto and:
a) relations between the organization and certificate Holder are modified or severed for any reason;
b) cases have arisen involving wlllful malice and/or disloyalty by the employee for which the organization requested the Certificate;
c) the right, position or role inherent to the powers of representation or the professional qualification pursuant to which the certification was issued has been lost.
The Certifier shall notify the Certificate Holder of the revocation and/or suspension request made by the "interested third party". Actalis may reject the request if it deems it to be inauthentic, inaccurate or incomplete and shall notify the requesting "interested third party" of the rejection.
17.6 In any case, the Certifier shall have the right to suspend/deactivate the certificate in the event of tampering with the certification keys or if it believes that the Manual procedures have been violated. In the event of Certificate revocation, for any reason, none excluded and/or excepted, the Customer shall not be entitled to the return of the amount paid.

18. Disclosures pursuant to art. 5, 52, 53, 64 et seq. of Legislative Decree 206/2005 and pursuant to art. 7 of the Legislative Decree 70/2003

18.1 In accordance with the provisions of articles 5, 52, 53, 64 et seq. of Legislative Decree 206/2005, the Customer acknowledges that:

a) The Supplier is Actalis S.p.A. headquartered at Via San Clemente 53 24036 Ponte San Pietro (BG), REA [Economic and Administrative Index] 445886, VAT Reg. 01879020517;
b) The Customer acknowledges and accepts that the Digital Signature Device, consisting of the provision of a customized product, falls under the provisions in art. 55 of Legislative Decree 206/2005 and that, as such, in accordance therewith and with the provisions of Law 40/2007, the exercise of the right to withdraw is not permitted, as indicated in Art. 16 above. The order may be halted and possibly cancelled, by written communication sent by registered letter with confirmation of receipt to Actalis S.p.A., Via San Clemente 53 24036 Ponte San Pietro (BG), only if the production relating thereto has not yet been commenced in any way; in such case, the Customer shall be entitled to obtain exclusively the return of the fee paid;
c) any complaints may be sent to the Certifier, by certified email (PEC) or registered letter with confirmation of receipt, to the respective registered offices;
d) the technical support service established for the individual services is described in art. 11 above.

19. Final provisions and communications

19.1 The relations between the Certifier and the Customer established in these General Conditions may not be deemed to constitute an agency, partnership, proxy, employment or association or any other similar or equivalent contracts.
19.2 No amendment, footnote or clause howsoever added to this contract shall be valid unless specifically and expressly approved in writing by all contractual parties.
19.3 All notifications to the Customer relating to this contract may be carried out by the Certifier by hand, via e-mail, by means of registered letter with return receipt, ordinary post or by fax to the addresses indicated by the Customer and, consequently, such notifications shall be considered known by the former. Any changes to the Customer's addresses not notified to the Certifier may not be raised against them [sic]**.**
19.4 Any total or partial ineffectiveness and/or invalidity of one or more clauses of the contract shall not result in the invalidity of the other clauses, which shall be deemed to be valid and effective. A null or inapplicable provision shall be interpreted in the closest manner possible to the parties' intentions.
19.5 Any claims concerning the supply of the Digital Signature Device ordered by the Customer shall be sent to the Certifier, by certified email (PEC) or registered letter with confirmation of receipt, to the respective registered offices. The Certifier shall consider the complaint and provide a written reply within 60 (sixty) days from receipt thereof. In the event of complaints due to particularly complex circumstances, which do not permit a full reply within the time limits referred to above, the Certifier shall notify the Customer within the afore-mentioned deadlines on the progress of the case.
19.6 The Contract is entered into in the Italian language; any other foreign-language versions are made available to the Customer exclusively as a courtesy. In the event of conflict, the provisions contained in the Italian version shall prevail over the others.

20. Applicable Law

For anything not expressly provided for in these General Conditions, reference shall be made, as far as compatible, to the Italian legal provisions currently in force upon the execution of the contract.

21. Competent Court

For any and every dispute relating to the interpretation, performance and termination of this Contract, the Court of Arezzo will have

exclusive jurisdiction, except in the event that the Customer has acted and entered into this Contract in the capacity of Consumer for purposes other than business or professional activities, in which case, the Court of the location where the Customer resides or is domiciled, if located in Italy, will have exclusive jurisdiction.

22. Processing of personal data

22.1 Processing of the Customer's personal data, for the purposes of signing the Contract and the subsequent provision of the Service, will occur in compliance with Legislative Decree 196/2003, Regulation (EU) 2016/679 and the privacy policy available at https://www.actalis.com/documents/tc-files/it/it-privacy-policy-actalis.aspx.

22.2 As a result of signing this Contract, relating only to data entered and/or submitted by the Customer which are processed exclusively in the context of the following Services, indicated in the Financial Offer which, depending on the case, may be available to the Customer (in the case of a direct purchase) or the C.D.R.L. (in the case of a resale):

- REMOTE SIGNATURE:
  - ARSS Cloud as a service;
  - Dedicated in the cloud
- ASB AUTOMATIC SIGNATURE - R:
  - as a service;
  - installed in the Cloud managed by the Supplier.

The Customer appoints Actalis as Data Processor of the personal data provided by the Customer, as described in Article 23 below.

23. Appointment of the Data Processor

For the Services under this Contract that specifically require it, the Customer appoints Actalis as Data Processor pursuant to art. 28 of Regulation (EU) 2016/679, in accordance with the detailed description of the tasks and duties assigned to it for this role and in accordance with the following.

This appointment as Data Processor and the related clauses shall have the same duration as the Contract signed between the Customer and Actalis in connection with the chosen Service.
The appointment and this document shall automatically cease to have effect in the event of the termination, withdrawal or loss of effectiveness of the Contract, except when time is needed for the Customer to retrieve personal data as contractually agreed between the parties.
Likewise, in the event of automatic Contract renewal, the appointment as Data Processor shall be deemed automatically renewed for a term equal to that of the contract.

I. Data processed by Actalis in the provision of the services pursuant to the Contract
The Services provided by Actalis, in accordance with their Technical Specifications, allow the Customer to process the data in accordance with the timescales and procedures set forth and independently managed by them, without prejudice to the applicable regulations. The scope of Actalis' appointment relates solely to the processing of personal data entered and/or provided independently by the Customer through the chosen Service and/or within the scope of that Service, and in any event in compliance with the purposes defined for its correct delivery by the Suppliers and in accordance with the provisions of the applicable regulations in force at any given time.
It is understood that, pursuant to and for the purposes of Legislative Decree 70/2003, in its provision of the Services, Actalis is neither responsible for the information stored at the Customer's request, nor subject to a general obligation to monitor the information it transmits or stores, or to a general obligation to actively seek to identify facts or circumstances that would indicate the presence of unlawful activities.

II. Obligations and rights
As a result of this appointment, Actalis is authorised solely to process the personal data to the extent necessary for performing the activities assigned to it. Actalis is entitled to undertake all activities necessary for ensuring fulfilment of the current relevant provisions as well as the task of organising, managing and supervising all processing operations for the personal data submitted to it by the Customer for the purposes of performing the activities covered by the chosen Service. In compliance with the provisions of Regulation (EU) 2016/679 and the regulations concerning the processing of personal data, it is specified that Actalis has the following obligations:

a) to process the personal data entered and/or submitted, in a lawful, correct and transparent manner, within the scope of execution of the chosen Service under the Contract, with the technical and security characteristics established on the basis of the provisions thereof, in the Manuals, in the Technical Specifications governing them and in the Codes of Conduct to which Actalis has subscribed in relation to the chosen Service, which for the purposes of this article must be regarded as documents containing instructions for the processing of data accepted by the Customer. In the event that the Customer expresses particular needs that require different instructions from the ones described in the aforementioned documents, he/she must demonstrate such need to Actalis and describe the measures that need to be guaranteed, which will be evaluated and, if feasible, quoted with a specific offer;
b) to ensure that the persons authorised to process the personal data have committed to confidentiality or have an adequate duty of confidentiality; Actalis shall specifically assign those persons who are authorised for data processing in connection with performance of the aforementioned activities, and shall provide them with the necessary instructions and inform them with the agreed methods and those prescribed by Regulation (EU) 2016/679;

c) to adopt all the technical and organisational measures required by Article 32 of Regulation (EU) 2016/679; in particular, in its provision of the chosen Service, Actalis shall implement the measures specified in the Contract, in the Technical Specifications, in the Manuals relating to the Service itself and in the Codes of Conduct to which it has subscribed in relation to the chosen Service, as well as the procedures adopted by the same in accordance with the ISO 27001 standard;
d) taking into account the nature of the data processing, to assist the Customer (i) with appropriate technical and organisation al measures, to the extent possible, in order to respond to requests received for exercising of the Data Subjects' rights; (ii) so as to ensure compliance with the obligations set out in Articles 32-36 of Regulation (EU) No. 2016/679, also taking into account the information available to the data processor;
e) at the Customer's request, to delete or make available all the personal data to the latter, once provision of the processing-related services has come to an end, and to delete any existing copies;
f) to make available to the Customer all the information necessary for demonstrating compliance with the obligations relating to the appointment set forth in this document, so as to enable and facilitate the revision and verification activities, subject to agreement with regard to timing and methods, and provided they are not in conflict with confidentiality obligations accepted by Actalis and/or with its policies. The costs of these checks will be borne by the Customer. Accordingly, Actalis shall process the data in compliance with the aforementioned instructions, the guidelines in the Manual governing the Service, any attachments and the provisions of Regulation (EU) 2016/679, and in compliance with the security requirements established for provision of the individual services.

III. Sub-processors

By signing this document, the Customer authorises Actalis to use its own sub-processors, as well as third-party suppliers and companies belonging to the Aruba Group for the provision of services (support, maintenance, the provision of additional services, network providers and electronic communication services) in connection with the requested service; the Customer acknowledges and accepts that this may entail the processing of data by said parties.
For the purposes of the appointment of a sub-processor, Actalis guarantees, by means of a written contract, that:

a) the sub-processor undertakes to process the Customer's data in a lawful, correct and transparent manner, in compliance with the provisions of Regulation (EU) 2016/679 and other rules on the processing of personal data and to the extent required to fulfil the obligations delegated thereto under the Contract;
b) the sub-processor shall accept the obligations pursuant to Article 28 of Regulation (EU) 2016/679;
c) Actalis shall remain liable to the Customer for all the obligations accepted, including those relating to the activities entrusted to the sub-processor.

In order to provide the Customer with precise control over the aforementioned third parties, in addition to complying with the requirements applying to the entire category of such third parties, Actalis undertakes to keep up to date the list of said third parties as well as the appropriate documents stating the obligations accepted by said third parties in relation to the duties arising from the processing of the personal data specified herein, where they process data within the context of the chosen Service.
If requested, Actalis undertakes to notify the Customer in the event of any changes made to such third parties.

IV. Breaches

Should any events occur, involving a breach of the personal data processed by Actalis in its provision of the Services, the latter shall notify the Customer in the manner and within the timescales stipulated in current applicable legislation on the subject.

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Registration no. 03358520967 | **TAX ID registration No.**03358520967
REA [Economic and Administrative Index]] 436479 | **Share Capital.** € 6.300.000,00 fully paid in|