This document defines the general conditions for the use of Pass'IN certificates offered by IN Groupe.

Definitions:

Customer:	refers to the entity that is a legal entity that purchases a certification service from Pass'IN Certification Authorities (CAs).
Information:	refers to the information to be published by the Supplier, namely the list of revoked certificates, the certification policy, the general terms and conditions of use and the certificates of the Certification Authorities
Party (Parties):	refers alternately or collectively to the Customer and the Service Provider
Subscriber:	refers to a natural person, employee, staff member or co-worker of the Customer
Service Provider:	refers to IN Groupe in its capacity as a Trusted Service Provider

1 TSP contact info

Requests for information:

IN Groupe - Responsable de l'AC
38 avenue de New York
75016 Paris
contact.passin@ingroupe.com

Revocation requests:

Online, by the Subscriber himself/herself at the address https://crl.pass-in.fr/ after identification with his/her card

By a **phone call to** the call centre (0820 670 314) providing its set of questions and answers

By **mail/e-mail** by sending the revocation request form available on the portal at https://crl.pass-in.fr/ to the following address: IN Groupe - Service Autorité d'Enregistrement - TSA 21006 - 59359 Douai cedex - France; or to the following address: passin.revocation@ingroupe.com

2 Certificate type, validation procedures and usage

Certificates issued by Pass'IN CAs can only be used for authentication and/or signature purposes in paperless exchanges.

The signature of a document with a signature certificate, in addition to (i) the authentication of the signatory (ii) the integrity of the data thus signed and (iii) the origin of the document, also provides a convincing guarantee of its date and the signatory's consent as to its content.

Certificates are issued for a period of 3 years, unless revoked.

The Customer is committed to ensuring that the Subscribers comply with these provisions.

3 Reliance limits

The use of these certificates is prohibited:

- ➲ beyond their validity period;
- ➲ if they have been previously revoked;
- ➲ if the Pass'IN CAs that issued them have ceased their activity;
- ➲ For any use other than those authorised by the Certification Policy (CP), as listed under "Area of Application of the Certificates".
- ➲The Customer guarantees that the Subscribers shall comply with these provisions.

4 Obligations of subscribers

The Subscriber has a duty to: (1) provide accurate and up-to-date information at the time of registration and renewal applications; (2) sign and comply with the PDS provided to it at the time of registration; (3) use certificates issued by IN Groupe only for authentication and signature purposes in accordance with the Certification Policies of the Pass'IN CAs; (4) apply the certificate protection policy defined in the certificate user guide provided to each Subscriber with their initial certificate; (5) protect his/her private key by means appropriate to his/her environment; (6) protect the activation data of the corresponding key pair with a PIN code; (7) protect access to the workstation on which his/her certificate is installed; (8) inform the CA of any changes to the information contained in its certificate; (9) promptly request revocation of its certificate directly to the Registration Authority (RA) or CA in the event of compromise, suspected compromise, theft, loss of private key, non-compliance with these PDS; (10) Stop all use of the certificate and the associated private key, in the event of termination of the CA's activity, or revocation of the CA's certificate by the IN Groupe, regardless of the cause of revocation; (11) The acceptance of the certificate by the Holder is carried out explicitly by signing an agreement during the activation phase of his/her card and returns it to the RA who will keep it. It is the Holder's responsibility

to check the consistency of the information contained in the certificate. It should also be noted that any certificate for which the RA has not received proof of acceptance by the Subscriber within 40 days of receipt of the card will be revoked by the CA.

5 Certificate status checking obligations of relying parties

Users of certificates must: (1) Check the use for which the certificate was issued; (2) Check that the certificate used was issued by a Pass'IN CA; (3) Check that the certificate is not present in the revocation lists of the corresponding CA; (4) Check the signature of the certificate, and the certification chain, up to the "ROOT" CA that issued the certificates of the Pass'IN CAs and check the validity of the certificates

6 Limited warranty and disclaimer/Limitation of liability

The Pass'IN CAs guarantee:

- Their identification and authentication through their certificate signed by the Root CA;
- The identification and authentication of Subscribers through the certificates they issue to them;
- Management of the corresponding certificates and certificate validity information according to the applicable CPs.

These warranties are exclusive of any other CA warranty.

It is expressly understood that IN Groupe cannot be held liable for any damage resulting from the fault or negligence of a Customer and/or its Subscribers or for any damage caused by an external event or force majeure, in particular in the event of:

- Use of the private key for a purpose other than that defined in the associated certificate, the CP, and the PDS;
- Using a certificate for an application other than Authorised Applications;
- Use of a certificate to guarantee an object other than the identity of the Subscriber;
- Use of a revoked certificate;
- Incorrect storage methods for the private key of the Subscriber's certificate;
- Using a certificate beyond its validity limit;
- Events external to the issue of the certificate such as a failure of the application for which it can be used;
- Force majeure as defined by French legislation.

The CA can only be held liable in the cases listed exhaustively below (subject to the Customer's compliance with the obligations imposed on it, and in particular those delegated to the Certification Agent):

- in the event of proven direct damage to a Subscriber or an application/certificate user as a result of a breach of the procedures defined in the CP and associated CPS, the CA's fault must be duly proven;
- in the event of proven compromise, entirely and directly attributable to the CA.

The CA disclaims any responsibility for the use of certificates issued by it under conditions and for purposes other than those provided for in its CP and any related applicable contractual documents, in particular:

- use of a certificate for a purpose other than authentication and signature of the Subscriber or protection of electronic mail;
- use of a certificate to guarantee an object other than the identity of the Subscriber for whom it was issued;
- use of a revoked certificate;
- use of a certificate beyond its validity limit.

The CA cannot be held liable for the consequences of delays or losses in the transmission of any electronic messages, letters, documents, and for any delays, alterations or other errors that may occur in the transmission of any telecommunications.

The CA also disclaims liability for any damage resulting from errors or inaccuracies in the information contained in the certificates, where such errors or inaccuracies result directly from the incorrect nature of the information provided.

The CA cannot be held liable, and shall not assume any liability, for any delay in the performance of obligations or for any failure to perform obligations resulting from its CP when the circumstances giving rise to them and which could result from the total or partial interruption of its activity, or from its disorganisation, fall within the scope of force majeure within the meaning of Article 1218 of the *Code civil* (French Civil Code).

In addition to those usually retained by French court case law, labour disputes, the failure of the network or external telecommunications installations or networks are expressly considered to be force majeure or unforeseeable circumstances.

The CA disclaims any liability for indirect damages (including financial or commercial damages) which, as a result, do not give rise to any right to compensation.
In any event, any compensation that IN Groupe as a CA may be required to pay in respect of a proven breach of its obligations may not exceed the amount(s) defined in the service contract.

7 Applicable agreements, CPS, CP

The identifiers of the CP applicable for these PDS are:

- Individual Substantial CA: 1.2.250.1.295.1.1.8.6.1.101.1, 1.2.250.1.295.1.1.8.6.1.102.1, 1.2.250.1.295.1.1.8.0.1.101.0 & 1.2.250.1.295.1.1.8.0.1.102.0
- Individual High CA: 1.2.250.1.295.1.1.20.7.1.102.1 & 1.2.250.1.295.1.1.20.0.1.102.0

8 Privacy policy

The personal data collected by the CA for the performance of the Services may be collected directly from the person concerned or indirectly from the Customer's legal representative or the certification agent.

In accordance with the provisions of law no. 78-17 of 6 January 1978 as amended, relating to data processing, files and freedoms, as well as the provisions of EU General Regulation 2016/679 of 26 April 2016 on Data Protection, the persons concerned by the collection of personal data are informed that:

➲ The data controller is IN Groupe in the context of issuing Pass'IN card.

➲ The data are processed by IN Groupe in order to produce the Pass'IN card and to ensure its lifecycle (renewal, revocation…)

➲ The CA collects and processes information on natural persons identified in the Pass'IN card applications in order to obtain certificates. These are the Holder, the certification agent, the Customer's legal representative and the contacts for invoicing the Customer.

➲ The processing is carried out on the basis of the contract signed between the Parties and in accordance with the Regulation (EU) 910/2014 and the related standards EN 319 401, EN 319 411-1 and EN 319 411-2, laying down the requirements for the qualification of authentication and signature certificates, and the qualification of services for issuing qualified electronic signature certificates.

➲ The data collected is stored in processing for a period of 12 months at the end of the validity period of the Pass'IN card. Pass'IN card application files are archived outside data processing for 10 years, in accordance with the requirements of Regulation (EU) 910/2014.

➲ The data subject also has the right to lodge a complaint with the certificate authority (see TSP contact info) if he/she considers that the processing operation concerning him/her constitutes a breach of the applicable regulations on the protection of personal data.

➲ All the data collected is necessary to produce the Pass'IN card, to send it and to send its activation code to its Subscriber in accordance with the processes described in the Certification Policies. If any of the data is missing or absent, the Pass'IN card will not be issued.

The data collected will only be processed for the purposes for which it was collected.

The CA states and guarantees that the collection of personal data under this agreement and the processing for which it is responsible are carried out in accordance with the provisions of the applicable data protection regulations.

The CA shall ensure the confidentiality and security of the data collected hereunder. The CA shall implement appropriate technical and organisational security measures to protect the data. The data shall only be disclosed to those who need to access it as part of the performance of the services.
The data may be transmitted to the CA's technical operator, which complies with the same privacy policy as the CA.

9 Refund policy

Refund policies are defined by the general terms and conditions of sale attached to the order or by a specific contract between the service provider and the customer.

10 Applicable law, complaints and dispute resolution

The law applicable to the PDS is French law.

In the event of a difficulty in performing the PDS and prior to referring it to the competent court, the Party first taking action will send a registered letter with acknowledgement of receipt to the other Party describing the dispute that has arisen between the Parties (hereinafter referred to as the "**Dispute**") and requesting the setting up of a amicable settlement procedure of the Dispute, which will take place as follows:

- within ten days of the receipt of this letter, the representatives of each of the Parties must meet in order to find an amicable outcome to their Dispute,
- the amicable settlement procedure cannot exceed sixty days from the receipt of the registered letter with acknowledgement of receipt describing the Dispute, except with the express agreement of the Parties to extend this period,
- all the information exchanged during this amicable settlement procedure will be considered to be confidential and shall be so, even if it does not mention confidentiality; the Parties can be assisted by their counsel, if they wish, during the amicable settlement meetings subject to notifying the other Party beforehand,
- the decisions made during this amicable settlement procedure have a contractual value, when an amendment or settlement agreement is signed by the authorised representatives of both Parties.

However, the Parties agree that they are not bound to apply the amicable settlement procedure before the implementation of interim, protective, summary or ex parte proceedings.

Failing amicable agreement, any dispute over the existence, validity, formation, implementation, interpretation or cessation of the Services and commercial relations falls under the exclusive competence of the *Tribunal de commerce* (commercial court) of Paris.
This clause also applies to interlocutory appeals, the introduction of third parties, additional claims or multiple defendants, and whatever the mode and manner of payment.

11 TSP and repository licenses, trust marks, and audit

A compliance check of the CP may be carried out at the request of the CA Supervisory Board and under the responsibility of the CA's Internal Audit Department (or department acting as such). As such, the CA may audit the compliance of the operations carried out by the Certification Agent.

The CA undertakes to carry out this audit at least once a year.

In addition, prior to the first commissioning of a component of its infrastructure or following any significant change within a component, the CA shall also have that component checked for compliance.

The Individual Substantial and Individual High CAs have also obtained qualification of their offering of electronic signature certificates with regard to the European eIDAS Regulations;
The Individual Substantial CA has also obtained compliance of its offering of electronic authentication certificates with regard to the ETSI EN 319 411-1 standard at NCP+ level.

Last name:	First name:
Date:	
CERTIFY THAT THEY HAVE READ AND ACCEPT THESE PDS	
Signature of the Subscriber :	