ID certificate request form

Your ID on the Internet

TBS Certificats reference number
1550229780

1 Certificate support

ID certificate delivered on support:

- ☐ Software
- ☒ USB cryptographic key
- ☐ Smart card + USB reader

2 Offer selection

Certificate type:

- ☐ Pack ID RGS*
- ☒ Pack ID RGS**
- ☐ Pack ID RGS***
- ☐ Chiffrement RGS*

Subscription (and certificate) duration of validity:

- ☒ a year
- ☐ 2 years
- ☐ 3 years

3 Information about the future holder

First Name Last Name:	Future HOLDER
E-mail:	future.holder@tbs-certificats.com

4 Information regarding the entity owning the certificate

Entity

Company name:	TBS CERTIFICATS		
Organisation number:	44044381000021		
Address:	22 rue de Bretagne		
Post Code:	14000	**City:**	CAEN
Country:	France	**Phone Number:**	+33-2-7630-5900

Function of the entity's future holder

Job Title:	Accountant

Entity legal representative

First Name Last Name:	Legal REPRESENTATIVE
E-mail:	legal.representative@tbs-certificats.com
Phone Number:	+33-2-7630-5900

5 Signature of the entity and of the future holder

The entity legal representative or by order, the CM designates HOLDER Future as future holder of the certificate, object of the present request.

Signature of the legal representative. Remain within the framework.

Date: 15/02/2019

Legal Representative

I, undersigned HOLDER Future

- certifies on honor the accuracy of the above information;
- being the certificate subscriber;
- certifies he read and understood the attached General terms of Use;
- accepts the role of certificate future holder, object of the present request;

Signature of the future holder. Remain within the framework.

Date: 15/02/2019

Future Holder

6 For Registration Authority use only

Operator:

Documents received:

- ☐ Only to addressee of:
- ☐ By post
- ☐ Other, please specify:

Notes:

Date and signature:

FORM TO RETURN

CERTIFICATES ISSUED BY « CERTIGNA IDENTITY PLUS CA »

1. OBJECT

The purpose of these conditions is to specify modalities of request and use of a « Certigna Identity Plus CA » certificate, proposed to a future Subject and/or a Subject, as well as the respective commitments and obligations of the related parties. The terms and conditions arise from the Certification Policy identified by the 1.2.250.1.177.2.3.1 OID available at the address: http://politique.certigna.fr/PCcertignaidentityca.pdf. Certificates covered by this Certificate Policy and these terms and conditions have the following OIDs:

- Certificates for company and administrative authority:
  - Authentication and signature Level ** : 1.2.250.1.177.2.4.1.1.1
  - Authentication Level *** : 1.2.250.1.177.2.4.1.2.1
  - Signature Level *** : 1.2.250.1.177.2.4.1.3.1
- Certificates for individual:
  - Authentication and signature Level ** : 1.2.250.1.177.2.4.1.4.1
  - Authentication Level *** : 1.2.250.1.177.2.4.1.5.1
  - Signature Level *** : 1.2.250.1.177.2.4.1.6.1

2. DEFINITIONS

- **CA**: « Certigna Identity Plus CA » Certification Authority of the DHIMYOTIS company, issuing the CERTIFICATE;
- **ROOT CA**: Higher level Authority of the Certigna PKI which certifies the CAs;
- **ISSUING CA**: Authority whom the certificate has been signed by the ROOT CA. The CA is an ISSUING CA in the Certigna PKI;
- **RA**: Registration Authority of DHIMYOTIS company controlling certificate requests and eventually revocation requests;
- **DELEGATED REGISTRATION AUTHORITY (DRA)**: Third party external to the PKI with which DHIMYOTIS has concluded a delegation contract by which it subcontracts part of the RA activity, namely, the collection and control of certificate requests, identification of certificate requesters and the submission of revocation requests;
- **CERTIFICATE**: Electronic certificate constituted of a file of electronic data signed, conforming to X.509 v3 standard, containing information on the SUBJECT;
- **CERTIFICATE REQUEST**: Set consisting of the request form (accepting the present General conditions of use) accompanied by the evidence documents, and the request generated by computer;
- **CERTIFICATION AGENT**: Person designated and placed under the responsibility of the Client entity. It is in direct contact with the RA and ensures for it a certain number of verifications concerning the identity, possibly the attributes of the SUBJECT and its entity.
- **CRYPTOGRAPHIC DEVICE**: USB key, smart card or cryptographic module;
- **CONTRACT**: Relations between the CA and the SUBJECT;
- **REISSUE**: Operation consisting in issuing a new CERTIFICATE in replacement of an existing one, with the same information but a different key pair (following the loss of the certificate or the password);
- **REVOCATION**: Operation consisting in anticipating the end of validity of a CERTIFICATE initially foreseen and the date of which is recorded in the CERTIFICATE;
- **SUBJECT**: Natural person for who the CERTIFICATE REQUEST has been accepted and processed by CA, and who is responsible for the CERTIFICATE and for the private key corresponding;
- **USER**: Certificate user.
  - For authentication certificate, it can be:
    - An online service that uses a certificate and an authentication verification device to validate an access request made by the certificate subject in the context of an access control or to authenticate the origin of a message or data transmitted by the subject of the certificate;
    - A user recipient of a message or data and who uses a certificate and an authentication verification device to authenticate the origin.
  - For signature certificate, it can be:
    - An online service that uses a signature verification device to verify the electronic signature on the data or a message of the subject of the certificate;
    - A user who electronically sign a document or a message;
    - A user recipient of a message or data and who uses a certificate and a signature verification device to verify the electronic signature by the subject of the certificate on this message or data.
  - For authentication and signature certificate, it can be the same users than an authentication or signature certificate.

3. COMPLIANCE

THE CERTIFICATE is issued in compliance with:

- the CP « *Certificats électroniques de Services Applicatifs* » for the authentication and/or signature usages at levels ** and *** of the « Référentiel Général de Sécurité » (RGS) developed by the National Agency for the information systems security (ANSSI);
- The eIDAS Regulation (EU) N°910/2014 and at :
  - ETSI EN 319 411-1 NCP+ level for authentication certificates level **;
  - ETSI EN 319 411-2 QCP-n-qscd level for signature and authentication certificates level ***;

4. DURATION

The CONTRACT is concluded for a period chosen by the future SUBJECT (maximum 3 years for individual and maximum 5 years for company and administrative authority) and starts the day of the CERTIFICATE issuance by the RA.

5. PRICE

Except with the prior written agreement of the CA, the pricing and payment conditions are as follows:

- The selling price of the CERTIFICATE is that defined in the price schedule available on request from the sales department of Certigna,
- The selling price of the CERTIFICATE must be paid at the CERTIFICATE REQUEST with one of the following means of payment:
  - credit card on the site https://certigna.fr;
  - bank transfer, attaching the receipt provided by the bank;
  - check payable to DHIMYOTIS,
  - cash for any amount not exceeding € 1000;
  - administrative order, for public institutions only, by attaching a purchase order on behalf of the Institution.
- REGENERATION of a software CERTIFICATE is free of charge during the 3 months following the issuance of the CERTIFICATE by the CA;
- UNBLOCKING of the CRYPTOGRAPHIC DEVICE in which the CERTIFICATE is eventually provided is invoiced;

Except with the prior written agreement of the CA, any CERTIFICATE whose sale price has not been paid in full may, either not be issued, or revoked after its issuance by the CA. In accordance to article L.441-6 of the French Commercial Code, in case of non-payment at the due date indicated on the invoice, without obligation to send a reminder, penalties will be applied for delay calculated on rate of 3 times the statutory interest rate in force on the due date of the invoice, and a lump sum indemnity of € 40 for collection charges.

6. OBLIGATIONS OF CERTIFICATE MANAGER

The SUBJECT has the following obligations:

- Request the CERTIFICATE by following all procedure steps provided on the website: https://www.certigna.fr.
- Provide accurate and up-to-date information during the request or renewal of the CERTIFICATE;
- Send to RA, if applicable to the DRA or to a Certification Agent of the entity, by hand or by post, the registration form generated at the time of the CERTIFICATE request online on the website: https://www.certigna.fr, the payment, as well as the evidence documents.
- Generate the key pair associated with the CERTIFICATE in a device or CRYPTOGRAPHIC DEVICE meeting the requirements of Chapter 11 of the Associated Certification Policy and at least qualified:
  - « QSCD » by ANSSI ;
  - « Standard » level by ANSSI for ** level certificates and at « Enforced » level for *** level certificates;
- Inform the RA in case of non-receipt of an e-mail confirming the CERTIFICATE REQUEST or REVOCATION request.
- Following receipt of an e-mail from the RA indicating the non-conformity of the request or that the request is incomplete, make the modifications within 7 calendar days after receipt of this e-mail.
- Accept explicitly the CERTIFICATE from its CERTIGNA customer area during the process of downloading the CERTIFICATE or by paper mail signed by the SUBJECT on the express request of the RA. In the event of explicit non-acceptance, the certificate is automatically revoked by the RA;
- Protect the private key associated with the CERTIFICATE for which he is responsible by means appropriate to its environment:
  - If the private key is stored on hard disk, it must create, for its protection, a complex password (consisting of a combination of at least 8 characters among digits, lowercase and uppercase letters, and Special characters).
  - If the private key is stored on CRYPTOGRAPHIC DEVICE, the SUBJECT must take all measures for the security of the latter. If this is the case, when the latter is initialized with a PIN whose value has been communicated to the future CARRIER, the latter must imperatively replace it with a personal PIN code which must not be communicated in any way to a third party. The SUBJECT undertakes to ensure the confidentiality of this PIN code, particularly when it is entered when it is required in a signature, authentication or encipherment process. In the case of use of a CRYPTOGRAPHIC DEVICE, the SUBJECT also undertakes to obtain from Dhimyotis or, where appropriate, from the manufacturer, the existence of a version of the CRYPTOGRAPHIC DEVICE driver compatible with The operating system of its workstation. It must also ensure compatibility before any updates to its operating system.

- Protect its activation data and, if necessary, implement it;
- Respect the conditions of use of the CERTIFICATE and of the associated private key mentioned in chapter 10 of this document;
- Inform the CA of any changes to the information contained in the CERTIFICATE;
- Immediately make a CERTIFICATE REVOCATION request for which it is responsible to the RA, the DRA to which the CERTIFICATE request has been made or, where appropriate, the Certification Agent of the entity, when one of the causes of revocation of Chapter 9 is encountered;
- Save the private key associated with the CERTIFICATE;
- Take all appropriate measures to ensure the security of the computer (s) on which the CERTIFICATE is installed. The SUBJECT is solely responsible for the installation of the CERTIFICATE;
- no longer use a CERTIFICATE and delete the associated key pair after the expiry or revocation of this CERTIFICATE;
- Inform RA of its departure from the entity;

7. OBLIGATIONS OF CA AND RA

The CA is under an obligation of means for all obligations relating to the management of the lifecycle of the CERTIFICATE it issues. The CA agrees to:

- Can demonstrate to the users of the CERTIFICATE that it has issued the CERTIFICATE for a given SUBJECT and that the corresponding SUBJECT has accepted the CERTIFICATE;
- Take all reasonable means to ensure that SUBJECT is aware of their rights and obligations with respect to the use and management of keys, certificates, and equipment and software used for PKI.
- Provide technical support service by phone during business hours;
- Provide an on-line consultation service at https://www.certigna.fr allowing third parties to verify the validity of the CERTIFICATE issued by the CA at any time (see chapter 12).
- Carry out any collection and use of personal data in strict compliance with the laws and regulations in force in France, in particular with respect to the CNIL and Article 226-13 (Ordinance 2000-916 Of 19 September 2000, article 3, Official Journal of 22 September 2000, in force on 1 January 2002) of the Penal Code.

The RA is committed to:

- Verify and validate CERTIFICATE and revocation requests;
- Generate and place at the disposal of the SUBJECT the CERTIFICATE within five working days in case the CERTIFICATE request is compliant and complete.
- Revoke the certificate within 24 hours if the REVOCATION is compliant and the requester is authenticated and authorized.

8. CERTIFICATE PUBLICATION

The SUBJECT CERTIFICATE is not published by the CA.

9. REVOCATION

The main causes of revocation are:

- The Subject information contained in its certificate is not in accordance with the identity or purpose in the certificate (eg, change in the identity), this before the normal expiry of certificate;
- The Subject did not comply with applicable Terms and Conditions of the certificate;
- The Subject, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under this CP;
- The Subject, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the Subject's private key and / or its support);
- The legal representative of the entity to which it belongs notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Subject did not comply with applicable Terms and Conditions of the certificate or the CA obtains evidence that the certificate was misused;
- The CA is made aware that a subject has violated one or more of its material obligations under the Terms and Conditions;
- The service information contained in its certificate is not in accordance with the identity or purpose in the certificate, this before the normal expiry of certificate;
- The Subject, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under the CP or the CPS;
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA signing the certificates is revoked (which results in the revocation of all valid certificates signed by the corresponding private key);
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.
- The die of the Subject or the cessation of activity of the entity attached to the Subject;
- An error (intentional or not) was detected in the registration files;
- The Subject's private key is suspected of being compromised, is compromised, lost or stolen (or possibly the activation data associated with the private key);
- For technical reasons (failure to send the certificate ...).

The revocation request can be made by:

- The SUBJECT;
- A legal representative of the SUBJECT entity, or if applicable a Certification Agent of that entity;
- The CA or the RA.
- The revocation request may be made:
- By signed letter, accompanied by a photocopy of an official identity document of the requester;
- Online, on the site https://www.certigna.fr from the customer area of the SUBJECT or the Certification Agent if applicable.

10. CONDITIONS OF USE OF CERTIFICATE AND ASSOCIATED PRIVATE KEY

- Authentication CERTIFICATE is used for:
  - Authentication of subjects on remote Subjects or to other people. It may be authentication in the framework of an access control to a Subject or an application, or authentication of data's origin as part of the electronic mail.
- Signature CERTIFICATE is used for:
  - Data electronic signature. Such electronic signature brings, besides the authenticity and integrity of signed data, the manifestation of consent of the signatory for the content of these data.
- Authentication and signature CERTIFICATE, the uses are the same than authentication or signature CERTIFICATE.

The CERTIFICATE is used for applications where security needs are strong (for level**) and very strong (for level***) given the risks that threaten them. In case of non-respect of the uses, the SUBJECT or its entity could be held liable.

11. OBLIGATIONS OF USERS

USERS must :

- Respect the authorized uses of the CERTIFICATE and the associated private key. Otherwise, their liability could be incurred.
- Verify, prior to its use, the status of the certificates of the whole of the corresponding certification chain via the means offered for the verification of the certificates cited below.
- If the Certigna ROOT CA certificate is not installed on the USER's machine, the USER must download it from the website https://www.certigna.fr , precisely at the following addresses:
  - http://autorite.certigna.fr/ACcertignarootca.crt ;
  - http://autorite.dhimyotis.com/ACcertignarootca.crt.

  The CA certificate can be downloaded from the following addresses:
  - http://autorite.certigna.fr/identityplusca.crt ;
  - http://autorite.dhimyotis.com/identittyplusca.crt.

12. CERTIFICATE STATUS CHECKING MEANS

To verify the certification chain, the USER of a CERTIFICATE can download the authority certificates (ROOT CA and ISSUING CA) from the website: https://www.certigna.fr. The ROOT CA certificate can already be installed on the workstation of the USER according to the software configuration. To verify the REVOCATION status of a CERTIFICATE, the CA periodically publishes the CRL and offers an information service on the revocation status of the CERTIFICATES (OCSP server, for On-line Certificate Status Protocol). This list of revoked certificates and these services are accessible for applications using certificates at the addresses contained in the CERTIFICATES:

To access the CRL :

- http://crl.certigna.fr/identityplusca.crl
- http://crl.dhimyotis.com/identityplusca.crl

To access the OCSP server:

- http://identityplusca.ocsp.certigna.fr
- http://identityplusca.ocsp.dhimyotis.com

13. LIMIT OF LIABILITY

The CA cannot be held liable if the private key associated with the CERTIFICATE is compromised. The CA shall under no circumstances be held responsible for any damage caused using the CERTIFICATE. The CA cannot be implicated by delays or losses that the transmitted data signed with the CERTIFICATE can be impacted. The CA cannot be held responsible for problems related to force majeure, within the meaning of the Civil Code. If a case of force majeure has a duration exceeding fifteen days, the SUBJECT will be authorized to terminate the CONTRACT and there will be no prejudice.

14. CONTRACT AND MODIFICATIONS

The CONTRACT cancels any previous commitment.

The SUBJECT agrees that during the term of the CONTRACT, the CA may modify the general conditions of use. However, the conditions accepted and signed by the

SUBJECT remain valid throughout the duration of the CONTRACT unless the SUBJECT explicitly accepts the new conditions issued and published by the CA on the website https://www.certigna.fr. In this case, a letter must be sent to the CA together with the new general conditions of use marked "read and approved", the date and signature of the SUBJECT. In the event of renewal of the CONTRACT (renewal of the CERTIFICATE at the end of its validity or after its revocation), the new CERTIFICATE is subject to the applicable general conditions of use.

15. TERMINATION

If one of the parties fails to fulfil one of the obligations arising from these general conditions, the other party may notify him of the performance of the said obligation. Failing that for the defaulting party to have executed within fifteen days of such notification, the other party may terminate the CONTRACT.

16. CONDITIONS OF REFUND

The CERTIFICATE command cannot be cancelled when the CERTIFICATE request is being processed. Any CERTIFICATE issued cannot be the subject of a refund request.

17. PRIVACY POLICY

Electronic certificate application files containing personal data are archived for at least seven years and as long as necessary for the purposes of providing proof of certification in legal proceedings, in accordance with applicable law. The personal identity information can be used as authentication data in the event of a request for REVOCATION.

In addition, DHIMYOTIS retains the personal data for a period of three years from the end of the commercial relationship with the customer and 3 years from the last contact with the prospect. The delay starts from the last connection to the customer account or the last sending of an email to customer service, or from a click on a hypertext link of an email sent by DHIMYOTIS, a positive response to an email requesting if the client wishes to continue to receive commercial prospecting at the end of the three-year period.

In accordance with the law n ° 78-17 of January 6, 1978 relating to data, files and freedoms, modified and the European regulation "2016/679 / EU of April 27, 2016" relating to the protection of natural persons to the processing of personal data and the free movement of such data, you have the right to access, oppose, rectify, delete and portability of your personal data. You can exercise your right by sending an email to: privacy@certigna.com, or by mail to the following address: DHIMYOTIS, DPO Service, 20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France.

18. ASSIGNMENT OF THE CONTRACT

The SUBJECT cannot assign its rights to the CONTRACT.

19. DISPUTE RESOLUTION

The CONTRACT is subject to French law. Parties undertake to try to resolve amicably any dispute which may arise between them, either directly or through a mediator, within 2 months of receipt of the letter with acknowledgment of receipt of the dispute. Half of the costs of mediation shall be borne by each of the parties. If necessary, the case will be brought before the Commercial Court of Lille.

20. DHIMYOTIS CONTACT INFORMATION

Dhimyotis S.A.
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq, FRANCE
Phone : +33 320 792 409 - Fax : +33 956 952 412
Email : contact@dhimyotis.com

Future Holder
2019/02/15

Future Holder


RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ N° :
Nationalité Française
Nom : Representative
Prénom(s) : Legal
Sexe : M
Né(e) le :
à :
Taille : 1,82m
Signature du titulaire :
IDFRAA63666 <<<<<<<<<<<<<<<<<<<91111
J4777AAAC777AAAC J477 <<J4777AAAC777A


RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ N° :
Nationalité Française
Nom : Holder
Prénom(s) : Future
Sexe : M
Né(e) le :
à :
Taille : 1,82m
Signature du titulaire :
IDFRAA63666 <<<<<<<<<<<<<<<<<<<91111
J4777AAAC777AAAC J477 <<J4777AAAC777A

Insee
Mesurer pour comprendre

Service Info Sirene
09 72 72 6000
prix d'un appel local

Service Statistique
Répertoire SIRENE

Toute modification (changement d'adresse, statut, raison sociale, activité...) concernant votre entreprise doit être déclarée au CFE dont vous dépendez.
Pour plus de précisions, consulter le site internet Insee.fr à l'adresse :
https://www.insee.fr/fr/information/1972060

SITUATION AU REPERTOIRE SIRENE

A la date du 14 février 2019

Description de l'entreprise	**Entreprise active au répertoire Sirene depuis le 01/10/2001**
Identifiant SIREN	440 443 810
Identifiant SIRET du siège	440 443 810 00021
Désignation	TBS CERTIFICATS
Catégorie juridique	5710 - SAS, société par actions simplifiée
Activité Principale Exercée (APE)	6202A - Conseil en systèmes et logiciels informatiques
Appartenance au champ ESS	Non

Description de l'établissement	**Etablissement actif au répertoire Sirene depuis le 02/01/2007**
Identifiant SIRET	440 443 810 00021
Adresse	TBS CERTIFICATS TBS CERTIFICAT TBS INTERNET THAWTE ET 22 RUE DE BRETAGNE 14000 CAEN
Activité Principale Exercée (APE)	6202A - Conseil en systèmes et logiciels informatiques

Important :*A l'exception des informations relatives à l'identification de l'entreprise, les renseignements figurant dans ce document, en particulier le code APE, n'ont de valeur que pour les applications statistiques (décret n°2007-1888 du 26 décembre 2007 portant approbation des nomenclatures d'activités françaises et de produits, paru au JO du 30 décembre 2007).*
Avertissement :aucune valeur juridique n'est attachée à l'avis de situation.

Site de gestion: **INSEE, DR NORMANDIE**
SIRENE, Service Statistique
8 QUAI DE LA BOURSE
CS 21410
76037 ROUEN CEDEX 1

REPUBLIQUE FRANCAISE

Greffe du Tribunal de Commerce de Caen
Palais de Justice, Place Gambetta, CS 55445
14054 Caen Cedex 4

N° de gestion 2002B00090

Extrait Kbis

EXTRAIT D'IMMATRICULATION PRINCIPALE AU REGISTRE DU COMMERCE ET DES SOCIETES

à jour au 8 février 2019

IDENTIFICATION DE LA PERSONNE MORALE

Immatriculation au RCS, numéro	440 443 810 R.C.S. Caen
Date d'immatriculation	13/02/2002
Dénomination ou raison sociale	**TBS CERTIFICATS**
Forme juridique	Société par actions simplifiée
Capital social	220 000,00 Euros
Adresse du siège	22 Rue de Bretagne 14000 Caen
Activités principales	Fourniture, gestion, émission de certificats électroniques, achat, vente, location de biens immobiliers, conseil, production, programmation, intégration, systèmes informatiques.
Durée de la personne morale	Jusqu'au 12/02/2101
Date de clôture de l'exercice social	30 juin

GESTION, DIRECTION, ADMINISTRATION, CONTROLE, ASSOCIES OU MEMBRES

Président

Nom, prénoms	DONNIO Jean-Philippe, Claude
Date et lieu de naissance	Le 27/05/1974 à Laval (53)
Nationalité	Française
Domicile personnel	22 Rue de Bretagne 14000 Caen

Vice-président

Nom, prénoms	FAVRAY Fabienne
Date et lieu de naissance	Le 15/02/1971 à Asnières-sur-Seine (92)
Nationalité	Française
Domicile personnel	8 Promenade de Sévigné 14000 Caen

Commissaire aux comptes titulaire

Nom, prénoms	BAREC Yves
Nationalité	Française
Domicile personnel ou adresse professionnelle	37 Rue Jules Siegfried 76600 Le Havre

Commissaire aux comptes suppléant

Nom, prénoms	SANNIER Catherine
Nationalité	Française
Domicile personnel ou adresse professionnelle	55 Rue des Jacobins 14000 Caen

RENSEIGNEMENTS RELATIFS A L'ACTIVITE ET A L'ETABLISSEMENT PRINCIPAL

Adresse de l'établissement	22 Rue de Bretagne 14000 Caen
Nom commercial	TBS CERTIFICAT, TBS INTERNET, THAWTE, PITUX
Activité(s) exercée(s)	Fourniture, gestion, émission de certificats électroniques, achat, vente, location de biens immobiliers, conseil, production, programmation, intégration, systèmes informatiques.
Date de commencement d'activité	01/10/2001
Origine du fonds ou de l'activité	Apport

R.C.S. Caen - 08/02/2019 - 13:04:29

Greffe du Tribunal de Commerce de Caen
Palais de Justice, Place Gambetta, CS 55445
14054 Caen Cedex 4

N° de gestion 2002B00090

Précédent exploitant	
Nom, prénoms	DONNIO Jean-Philippe
Numéro unique d'identification	408 480 218
Mode d'exploitation	Exploitation directe

Le Greffier

TRIBUNAL DE COMMERCE DE CAEN (Calvados)

FIN DE L'EXTRAIT

tbs certificats
Accélérateur de confiance !

Template of authority delegation for certificates requests

I, the undersigned "Legal Representative designated on the registration document" acting as President and designated as Delegator declare giving delegation to "Legal Representative of the form" designated as Delegatee to sign digital certificate requests on behalf of TBS CERTIFICATS.

This delegation is established for a period of 3 years from the date of its signature.

Done in Caen

On 2019/02/15

The Delegator
Legal Representative designated on the registration document

LegalRepresentativeOnRegistration

The Delegatee
Legal Representative of the form

FormLegalRepresentative

* underlined terms must be replaced

Certigna intervention form

Holder's identity validation form

TBS Certificats reference numbe
1550229780

1 Certificate information

Certificate type:

☒ Pack ID RGS** ☐ Pack ID RGS*** ☐ Cachet Serveur RGS**

2 Information about the future holder

First Name Last Name: Future HOLDER

E-mail: future.holder@tbs-certificats.com

Information about the entity

Company name: TBS CERTIFICATS

Number of SIRET: 44044381000021

Address: 22 rue de Bretagne

Post Code: 14000 **City:** CAEN

Country: France **Phone Number:** +33-2-7630-5900

3 Information about the operator charged with the face-to-face

Company name: TBS INTERNET

Authorized operators list:

Authorized Operator (authorized.operator@aed.com)

Address: 22 RUE DE BRETAGNE

Post Code: 14000 **City:** CAEN

Country: FR

5 Operator's signatures and future holder

I, the undersigned and RA/DRA operator, certify that I have authenticated the above certificate's holder during a face-to-face meeting.
I certify that I have controlled this certificate holder's ID.
I certify that all of the information above is identical to what is found on the certificate holder's original ID.

Date, name and signature of the DR/DRA:

2019/02/15 Authorized Operator

I, the undersigned, HOLDER Future, certificate holder, certify having done my face-to-face interview.
I confirm that my PIN code will be modified prior to using the certificate if the latter wasn't modified during the face-to-face meeting.

Date and signature of HOLDER Future:

2019/02/15 Future Holder

As a reminder, you will have to present a valid official identity document (National Identity Card, passport, residency permit).

TO SEND BACK

Listing of required documents needed for an RGS certificate

Please follow this guide and tick the boxes to make sure you did not forget anything before sending us your documents.

1. Complete and sign the order form

On the copy TO BE RETURNED:

- ☐ HANDMADE signature of the legal representative or of the person with delegation of authority, with the "Read and Approved" words
- ☐ HANDMADE signature of the future holder with the "Read and Approved" words

Signature stamp won't be accepted.

2. Read and sign the "User's Terms and conditions"

On the copy TO BE RETURNED:

PAGES 1 & 2:

- ☐ Initials of future holder in the bottom of the first two pages

PAGE 3:

- ☐ Enter the FIRST and LAST NAMES of the future holder
- ☐ Add the date of T&C acceptance
- ☐ HANDMADE signature of the future holder

3. Photocopy an ID of the legal representative

Only acceptable: CURRENTLY VALID passport or ID card.

The ID must contain a picture and be photocopied double-sided.

4. Photocopy an ID of certificate future holder

Only acceptable: CURRENTLY VALID passport or ID card.

The ID must contain a picture and be photocopied double-sided.

5. Please gather the documents to be sent:

- ☐ The 4 documents described above
- ☐ Copy of a SIREN situation extract (LESS THAN 3 MONTHS OLD)
  Available on "http://avis-situation-sirene.insee.fr"
- ☐ A document proving the legal representative's status

- For a company listed on the commerce register:
a KBIS extract including the name of the organisation's legal representative.
- For a city or a community of cities:
the official report of the mayor and the deputies election or the official report of the community counsel election.
- For a charity:
The report of the board of directors' meeting designating the board members signed by at least two of them indicating their name, first name and job title above their signature.
- For a public organization::
The document concerning the nomination of the legal representative by his supervision authority.

In case of authority delegation (from a president to a director, for example):
It is the person having delegation that must be named in the form as Legal Representative.

- ☐ The photocopy of the ID of the person having delegation (as indicated in step 3 above)
- ☐ A valid document holding delegation (with both the signatures of the person giving delegation and the one receiving it) AND:

- For an administration (city, state, province...):
the minutes of the Legal Representative's election which signed the delegation document and shows his own signature
- For a company listed on the commerce register:
A full KBIS showing the name of the Legal Representative which signed the delegation document

6. Send these documents by post

Send all these documents:

- By post to: TBS Certificats - Certificates services / / 22 rue de Bretagne / / 14000 / CAEN / FR

Warning! Any document, signature, mention or missing date will delay your certificate issuance.
Thanks for your attention.