Processus 2D-Doc

Historique des versions

Version	*Date*	*Contributeur*	*Validateur*
0.6	29 avril 2012	Cyril Murie	Cyril Murie
0.7	9 mai 2012	Denis Pinkas	Cyril Murie
0.8	4 juin 2012	Cyril Murie	Cyril Murie
1.0	20 juillet 2012	Cyril Murie, AriadNEXT	Cyril Murie
1.01	9 octobre 2012	Cyril Murie	Cyril Murie
1.2	11 août 2020	David Lecornu	David Lecornu

Fonds documentaire

- **[Proc. 2D-Doc] :** Présent document. Ce document chapeau décrit les processus fonctionnels du projet, les apports nécessaires des autres documents, précise les spécifications techniques ne nécessitant pas un document spécifique.
- **[Document de gouvernance] :** décrit les mécanismes organisationnels et juridiques.
- **[Spec CAB 2D-Doc]** : décrit les caractéristiques techniques des codes à barres de type 2D-Doc.

Références

- **[REF DGME] :** Cahier des charges pour le référencement des produits de sécurité et des offres de prestataires de services de confiance, DGME.
- **[RGS] :**Référentiel Général de Sécurité, version 1.0 du 6 mai 2010, ANSSI, DGME.
- **[ETSI TSL] :** Spécification ETSI TS 102 231 qui traite des questions d'établissement, de publication, d'accès, d'emplacement, d'authentification et de confiance relatives aux listes de type TSL

Commentaires

Les commentaires sur le présent document sont à adresser à :
Agence Nationale des Titres Sécurisés
101, rue de Tolbiac
75013 PARIS CEDEX 13

En collaboration avec des entités privées et publiques, le ministère de l'intérieur met en place la solution « 2D-Doc » pour sécuriser les données échangées sous forme papier entre l'usager et l'administration.

Le standard code à barres bidimensionnel 2D-Doc consiste en la sécurisation de données dans un code à barres signé électroniquement par la clé privée correspondant à une clé publique placée dans un certificat du type « cachet serveur ». Pour un document, certaines données sont choisies, concaténées puis signées électroniquement. Les données et la signature sont mises en forme dans un code à barres spécifique de type 2D-Doc. Ce standard constitue une signature visible vérifiable uniquement par une machine. La différence majeure par rapport aux règles habituelles de signatures électroniques est l'absence du certificat dans le document signé, ceci pour des raisons de dimension du code à barres.

1. Architecture globale

Le processus 2D-Doc peut être découpé en étapes fonctionnelles simples :

- **Etape 1** : un participant émet un code à barres de type 2D-Doc, le met en forme sur un document et envoie celui- ci à un usager ;
- **Etape 2** : le participant envoie ce document sous format électronique ou papier à l'usager ;
- **Etape 3** : l'usager présente ce code à barres de type 2D-Doc à une administration qui vérifie alors son intégrité et sa conformité avec les données textuelles visibles sur le document.

1.1. Les rôles

Ce paragraphe a pour objectif de préciser de manière schématique les rôles dans le cadre du projet [2D-Doc] :

- **[MinInt]** : le Ministère de l'Intérieur dirige le projet 2D-Doc. Il référence les participants et dirige le comité de pilotage du programme [2D-Doc] ;
- **[ANTS]** : l'Agence Nationale des Titres Sécurisés assure le support technique du [MinInt] sur ce projet. Elle rédige les standards et met à disposition sur son site Internet les listes des [AC], des [Editeur]s et des [Participant]s, listes validées par le [Minint]. De manière générale, l'[ANTS] transmet des avis techniques au [MinInt], le [MinInt] transmet des décisions, les processus de décision sont décrits dans le [document de gouvernance] ;
- **[Participant]** : Personne morale mettant en place une solution d'écriture de code à barres [2D-Doc] sur les documents qu'elle émet ;
- **[Usager]** : Personne morale ou physique qui reçoit un document comportant un code à barres [2D-Doc] ;
- **[Utilisateur]** : Personne morale ou physique ayant fait le choix de lire les codes à barres de type [2D-Doc] pour avoir un élément d'information supplémentaire dans le cadre de la lutte contre la fraude.
- **[AC]** : Autorité de certification référencée par l'ANTS qui dans le cadre de ce projet émet des certificats de signature du type « cachet serveur » selon les standards [RGS], le niveau choisi est « * » (une étoile) ; l'[AC] peut être interne ou externe au [Participant].
- **[Editeur]** : Entité qui met en forme les données et la signature au format de code à barres « 2D-Doc ». L'Editeur travaille pour le compte d'un ou plusieurs participants. L'identité de l'Editeur n'est pas connue lors de la vérification d'une signature.

Les précisions nécessaires sur chacun des rôles sont apportées dans le document de gouvernance.

1.2. Les étapes fonctionnelles

1.2.1. Etape 1 : la création du code à barres

L'étape 1 peut être décomposée en étapes fonctionnelles simples :

- **Etape 1.01** : un candidat [participant] choisit une solution technique basée sur :
    - une [AC] référencée par l'ANTS ([AC] référencée par l'ANSSI ou référencement provisoire dérogatoire) ;
    - un [Editeur] référencé par l'ANTS.
- **Etape 1.02** : le candidat [participant] devient et reste un [participant]
- **Etape 1.03** : Le [participant] place, un code à barres de type [2D-Doc] sur le document. Le processus détaillé est le suivant :
    - les données à signer sont sélectionnées ;
    - ces données sont concaténées ;
    - la valeur de hachage est signée à l'aide de la clé privée correspondant au certificat du [participant];
    - les données et la signature sous la forme d'un code à barres 2D-Doc sont mises en forme ;
    - le code à barres est positionné sur le document.

1.2.2. Etape 2 : la mise à disposition du document

Le document est mis à disposition de l'[usager]. Cette étape ne nécessite pas d'être décomposée en étapes fonctionnelles.

1.2.3. Etape 3 : Le processus de lecture et de vérification

L'étape 3 peut être décomposée en plusieurs étapes fonctionnelles simples :

- **Etape 3.01** : l'utilisateur décode le code à barres et récupère l'identifiant de l'[AC] et l'identifiant du certificat ;
- **Etape 3.02** : à l'aide d'une TSL publiée sur le site de l'ANTS, l'[utilisateur] vérifie que l'identifiant de l'[AC] existe, puis récupère le certificat de l'AC, ainsi que l'adresse de l'annuaire où l'AC publie ses certificats ;
- **Etape 3.03** : l'[utilisateur] vérifie que ce certificat d'AC n'est pas révoqué ;
- **Etape 3.04** : l'[utilisateur] récupère le certificat du [Participant] correspondant à l'identifiant dans l'annuaire de l'[AC];
- **Etape 3.05** : l'[utilisateur] récupère la CRL de l'AC au point de distribution de la CRL indiqué dans le certificat du [Participant] et vérifie que ce certificat n'est pas révoqué ;
- **Etape 3.06** : l'[utilisateur] vérifie la signature numérique à l'aide de ce certificat ;
- **Etape 3.07** : l'[utilisateur] prend une décision sur la suite du traitement métier.

2. Analyse des Conditions requises

Cette partie décrit les différentes conditions requises liées à ces mécanismes.

2.1. Caractéristiques fonctionnelles

2.1.1. L'émission du code à barres

Etape 1.01 : un candidat [participant] choisit une solution technique basée sur une [AC] référencée par l'ANTS et un [Editeur] référencé par l'ANTS.
Ce choix fait par le candidat [participant] nécessite la mise à disposition d'une liste des [AC] référencées, et des [Editeur]s référencés.
Action(s)
Préciser le processus permettant à une entité de devenir et de rester une [AC] ou un [Editeur] référencés par l'ANTS : [Proc 2D-Doc]. Suite à ce processus, l'ANTS émet un avis [Minint] qui lui transmet la décision. Préciser le rôle des différentes entités pour ces référencements : [Document de gouvernance] Préciser le mode de diffusion de l'information : sur le site www.ants.interieur.gouv.fr. L'ANTS précise les raisons commerciales et les N° SIREN des entités référencée s dans un format lisible par un être humain.

Etape 1.02 : Le candidat [participant] devient et reste un [participant]
Une fois les caractéristiques de sa solution définie, le candidat [participant] doit connaître les règles qui lui permettent de devenir et de rester un [participant].
Action(s)
Préciser les conditions techniques pour devenir [Participant]: : le candidat soumet sa solution technique à l'ANTS qui émet un avis technique au [MinInt] qui lui transmet la décision prise. Préciser les conditions techniques pour rester [Participant]: lorsqu'informé d'un incident technique, l'ANTS émet un rapport d'analyse au [MinInt] qui lui transmet la décision prise. Préciser les conditions juridiques et fonctionnelles : [Document de Gouvernance].

Etape 1.03 : Le [participant] met en place un code à barres de type [2D-Doc] sur le document
Le [participant] a besoin de connaître les standards de ce code à barres pour mettre en forme les données de manière interopérable.
Action(s)
Préciser les caractéristiques techniques d'un code à barres de type « 2D-Doc » : [Spec CAB 2D-Doc].

2.1.2. La lecture de codes à barres

Etape 3.01 : Décoder le code à barres de type « 2D-Doc »
L'[utilisateur] doit être en mesure de décoder les codes à barres. Il récupère l'identifiant de l'AC, l'identifiant du certificat.
Action(s)
L'[utilisateur] doit être en mesure de décoder les codes à barres : [Spec CAB 2D-Doc]. L'[utilisateur] doit s'assurer de l'interopérabilité de la solution de lecture choisie : organisation de plugtests par l'ANTS.

Etape 3.02 : Récupérer l'adresse de l'annuaire de certificat de l'AC
A l'aide d'une TSL publiée sur le site de l'ANTS, l'[utilisateur] vérifie que l'identifiant de l'[AC] existe, puis récupère le certificat de l'AC, ainsi que l'adresse de l'annuaire où l'AC publie ses certificats.
Action(s)
L'[Utilisateur] doit connaître l'adresse de l'annuaire de l'[ANTS] : www.ants.interieur.gouv.fr L'[Utilisateur]doit pouvoir faire confiance en cette TSL. Pour cela, il vérifie la signature de la TSL. Elle doit être signée par une personne physique de l'ANTS dont le nom (DN) est disponible sur le site de l'ANTS accessible en mode HTTPS et la signature doit être vérifiée comme étant valide. La TSL est conforme au standard [ETSI TSL]. L'[Utilisateur] obtient dans un format lisible machine le certificat de l'AC, ainsi que l'adresse de l'annuaire où l'AC publie ses certificats: [Proc 2D-Doc].

Etape 3.03 : L'[Utilisateur] vérifie que ce certificat d'AC n'est pas révoqué.
A partir des éléments présents dans la TSL, l'[Utilisateur] vérifie le statut du certificat.
Action(s)
L'ANTS vérifie à chaque mise à jour le statut de chaque certificat d'AC mentionné dans la TSL selon le processus décrit dans le RFC 5280 (vérification du chemin de certification et vérification qu'aucun élément de ce chemin n'est révoqué). L'ANTS publie le statut du certificat dans la TSL.

Etape 3.04 : Récupérer le certificat du [Participant] correspondant à l'identifiant
A partir des éléments présents dans le code à barres 2D-Doc, l'[utilisateur] récupère l'identifiant d'un certificat du [Participant]. A partir de l'annuaire de l'[AC] et de cet identifiant, il récupère le certificat du [Participant].
Action(s)
L'[Utilisateur] utilise le protocole RFC 4387 pour récupérer dans un premier temps l'ensemble des certificats des [Participants] émis par cette AC. L'[Utilisateur] examine chaque certificat de [Participant] jusqu'à trouver celui dont l'attribut CommonName (CN) du champ « subject DN » contient l'identifiant du certificat du [participant] : [Proc 2D-Doc]. Un [Participant] peut avoir plusieurs certificats.

Etape 3.05 : Vérifier que le certificat du [Participant] n'est pas révoqué.
L'[Utilisateur] vérifie que ce certificat n'est pas révoqué.
Action(s)
L'[Utilisateur] récupère la CRL de l'AC au point de distribution de la CRL indiqué dans le certificat du [Participant] et vérifie que ce certificat n'est pas révoqué. L'[Utilisateur] vérifie que la CRL a bien été émise par l'AC et utilise le numéro de série du certificat du [Participant] pour savoir si ce numéro figure dans la CRL. L'[Utilisateur] obtient alors le statut du certificat, et si le certificat n'est pas révoqué, continue le processus.

Etape 3.06 : Vérifier la signature
A partir des éléments décodés du code à barres et du certificat récupéré, l'[utilisateur] vérifie la signature numérique.
Action(s)
L'[utilisateur] doit connaître le mécanisme de signature numérique utilisé : il ne s'agit pas d'une signature électronique selon l'un des formats normalisés par l'ETSI, mais d'une signature numérique appliquée sur des champs particuliers. La manière de calculer et de vérifier cette signature numérique est précisée dans le document [Spec CAB 2D-Doc].

2.2 Caractéristiques non-fonctionnelles

Condition Requise (CR) 4.01 : Disponibilité
Les [utilisateur]s doivent pouvoir avoir confiance en la disponibilité du système.
Action(s)
Le standard est une sécurité de niveau RGS « * ». Les règles de disponibilité liées au RGS « * » s'appliquent à l'ensemble du standard « 2D-Doc » y compris les différents annuaires. Définir les bonnes pratiques pour les [utilisateur]s : document [Proc 2D-Doc]

Condition Requise (CR) 4.02 : Interopérabilité
Les [Utilisateur]s et les [Participant]s doivent pouvoir s'assurer que les solutions sont interopérables.
Action(s)
Définir les règles permettant d'assurer l'interopérabilité : organisation de plugtest par l'ANTS.

Condition Requise (CR) 4.03 : Evolutivité
Les [Participant]s et [Utilisateur]s doivent pouvoir s'assurer que les évolutions de la solution prennent en compte les besoins d'évolutivité.
Action(s)
Décrire les modes de décision : [document de gouvernance].

Condition Requise (CR) 4.04 : Impacts légaux
Les [participant]s, les [utilisateur]s doivent avoir une connaissance des impacts légaux de l'utilisation de l'outil « 2D-Doc ».
Action(s)
La solution « 2D-Doc » est basée sur un mécanisme identique à celui de la signature électronique. Les règles de responsabilité sont donc celles du monde de la signature électronique .

2.3. Les annuaires

En conclusion de cette présentation fonctionnelle, les besoins sont listés ci-après. Ils sont scindés en trois parties :

1. les annuaires utilisés pour la vérification des signatures placées dans les codes à barres bidimensionnels,
2. l'annuaire consultable par les futurs [participant]s,
3. l'annuaire consultable par les AC référencées.

Annuaires nécessaires à la vérification des signatures placées dans les codes à barres

Liste des	*La liste référence la conformité*	*Identifiants utilisés*	*Responsable de la liste*	*Standard de publication de la liste*	*MAJ*
[AC] référencées	au [RGS] «*» sauf dérogations	Certificat d'AC Identifiant ANTS Adresse internet de l'annuaire de certificats émis par l'AC.	[ANTS] (où : www.ants.interieur.gouv.fr)	[ETSI TSL] Précisé par : [Proc. 2D-Doc]	MAJ : tous les 3 mois
Certificat de [Participant]	Au conditions de référencement des [participant]s par le [MinInt]	Certificat de [Participant] Identifiant [2D-Doc]	[AC] référencée (où : site internet de l'AC)	[selon RFC 4387] Précisé par : [Proc. 2D-Doc]	MAJ : à chaque nouveau certificat.

Annuaire consultable par les futurs [participant]s

Liste des	*La liste référence la conformité à*	*Identifiants utilisés*	*Responsable de la liste*	*Standard de publication de la liste*	*MAJ*
[Editeurs] référencés	[Spec CAB 2D-Doc]	SIREN Raison commerciale	[ANTS] (où : www.ants.interieur.gouv.fr)	Page Web : [Proc. 2D-Doc]	MAJ : tous les 3 mois

Annuaire consultable par les AC référencées

Liste des	*La liste référence la conformité à*	*Identifiants utilisés*	*Responsable de la liste*	*Standard de publication de la liste*	*MAJ*
[Participants] référencés	[Document de gouvernance]	SIREN/SIRET Raison commerciale	[MinInt] (où : www.ants.interieur.gouv.fr)	Page Web : Transposition via un fichier XSL d'un fichier XML : [Proc. 2D-Doc] [REF DGME]	MAJ : tous les 3 mois

3. Les référencements

Pour tous les référencements nécessaires, ce chapitre décrit :

- le processus de référencement ;
- le standard technique de la liste ;
- le mode de mise à disposition et la disponibilité.

3.1. Référencement ANTS des [AC]

Du point de vue de la sécurité, l'objectif de sécurité est tel que défini par le RGS pour les cachets serveurs de niveau « * ». Pour toutes les questions d'ordre technique, sécurité, légal, le projet « 2D-Doc » s'appuie sur un mécanisme spécifique de signature numérique et sur le Référentiel Général de Sécurité.

L'ANTS référence les certificats d'autorité pouvant émettre des certificats destinés à signer des codes à barres de type « 2D-Doc ». Ce référencement est réalisé à l'aide d'une TSL telle que définie par l'[ETSI TSL].

Pour permettre la mise en place rapide du projet, un mécanisme d'exception est prévu permettant de référencer une autorité de certification n'ayant encore pas subi la procédure d'accréditation par l'ANSSI.

3.1.1. Processus de référencement

3.1.1.1. Pour les aspects sécurité

Dans le cadre d'une procédure normale, l'autorité de certification a été accréditée par l'ANSSI pour émettre des certificats du type « cachet serveur » d'un niveau RGS « * ». Pour tous les aspects liés aux cachets serveurs, cette certification est suffisante.

Toutes les autorités de certification n'auront pas nécessairement subi l'audit d'accréditation de l'ANSSI. Dans ce cas, en plus de la procédure normale décrite dans le paragraphe précédent, le ministère de l'intérieur peut décider d'une procédure exceptionnelle permettant de référencer une telle autorité de certification. Cette procédure d'exception se justifie par le choix d'un [participant] de faire appel à cette autorité de certification non encore accréditée. Cette autorité de certification doit fournir un document décrivant la politique de certification (PC) mis en place pour assurer un niveau « * » ainsi que la DPC et l'engagement d'un [participant] pour utiliser cette autorité de certification.

3.1.1.2. Pour la gestion des certificats des [Participant]s

L'autorité de certification doit aussi montrer sa capacité à mettre en place un annuaire des certificats conformes aux standards définis dans ce projet : schéma conforme au RFC 4387. Cette démonstration se fait par une description des processus mis en place et des essais de lecture.

3.1.1.3. Transmission d'un avis

A partir de cette description papier des processus mis en place, des essais effectués et des mesures de sécurité, l'[ANTS] transmet un avis motivé au [MinInt]. En fonction de cet avis et du besoin de l'Etat français, le [MinInt] transmet sa décision à l'ANTS. L'ANTS référence alors cette autorité de certification et lui délivre un identifiant 2D-Doc sur quatre caractères : 2 caractères pour le code pays + 2 caractères.

3.1.1.4. Supervision et Processus d'exclusion

Lors de la vie du projet, l'[ANTS] a un droit de supervision, si l'autorité de certification ne respecte par ces obligations, l'[ANTS] transmet un avis motivé au [MinInt].

Le [MinInt] transmet à l'ANTS la décision prise sur le référencement de cette autorité de certification dans la TSL ANTS.

En cas d'incident critique, une processus d'urgence est mise en place et est décrite dans le « document de gouvernance ».

3.1.2. Caractéristiques techniques de l'annuaire des [AC]

Le modèle proposé de TSL est compatible avec une mise en œuvre fondée sur la spécification ETSI TS 102 231 qui traite des questions d'établissement, de publication, d'accès, d'emplacement, d'authentification et de confiance relatives à ce type de liste.

La TSL émise par l'ANTS est signée par un certificat au nom de l'ANTS avec le CN= ANTS CACHET 2DDOC et le numéro de série : 11219159e903cdd850d9c7073121b15104b9.

Elle comporte les informations suivantes pour chaque autorité de certification référencée :

- le certificat de l'AC conforme au gabarit X509V3
- les différentes informations habituellement contenues dans une TSL
- l'information sur la qualité de cette AC.
  Si l'AC n'a pas subi l'audit nécessaire pour être accrédité RGS « * », ceci est alors clairement précisé dans le champ « ServiceStatus ». Ce champ prend alors la valeur « inaccord ». Chaque [utilisateur] fait alors le choix de faire confiance ou non à cette autorité de certification. Le [MinInt] fait confiance à cette AC.
- l'identifiant ANTS (2 pour le code pays + 2 caractères) correspondant à l'AC dans le code à barres 2D dans le champ « TSPTradeName ». Cet identifiant est porté dans l'attribut commonName du DN du champ « subject » du certificat.
- l'adresse de l'annuaire des certificats délivrés par cette AC : cette adresse est dans le champ « TSPInformationURI » de l'AC de la TSL.

La signature de la TSL est vérifiable d'une part en utilisant la clé racine publiée sur le site de l'ANTS et d'autre part en vérifiant qu'elle est bien signée par la personne physique de l'ANTS dont le nom figure sur le site de l'ANTS.

3.1.3. Mise à disposition et disponibilité

- Cette liste est mise à disposition sur le site de l'ANTS : www.ants.interieur.gouv.fr
- La date de mise à jour est précisée dans la liste elle-même conformément au standard [ETSI TSL].

3.2. Référencement des [Editeur]s par l'ANTS

3.2.1. Processus de référencement

Pour être référencé, l'Editeur transmet à l'ANTS dix feuilles de test comportant un code à barres de types « 2D-Doc » pour des pseudo-participants. L'[ANTS] vérifie leur conformité au standard et transmet un rapport motivé au [MinInt]. Le [MinInt] transmet la décision à l'[ANTS].

3.2.2. Caractéristiques techniques de l'annuaire des [Editeur]s

Cet annuaire n'est pas lisible par une machine mais par un être humain. Le site comporte la raison commerciale de l' [Editeur], son numéro SIREN/SIRET.

3.2.3. Mise à disposition et disponibilité

Cette information est disponible sur le site de l'[ANTS] : www.ants.interieur.gouv.fr

Nota : cette information n'est pas utilisée durant le processus de vérification des signatures. Elle n'est utile que pour les futurs [participant]s à la recherche d'un Editeur.

3.3. Référencement des [participant]s par le [MinInt]

3.3.1. Processus de référencement

Le candidat [Participant] soumet 10 feuilles de test au [MinInt] avec des données différentes, le [MinInt] les remet à l'[ANTS]. L'[ANTS] transmet un rapport motivé au [MinInt].

Le [MinInt] référence les [participant]s au projet, référencement dont le processus est défini par le document de gouvernance. Techniquement, ce référencement est réalisé à l'aide de l'attribut organizationalUnitName tel que défini dans le standard [REF DGME].

3.3.2. Caractéristiques de l'annuaire des [Participant]s

Cet annuaire n'est pas lisible par une machine mais par un être humain. Il est maintenu par l'[ANTS] pour le compte du [MinInt]. Il est accessible en mode HTTPS.

Le [participant] a un statut au sein de l'annuaire, trois statuts sont possibles :

- *inaccord* : le [Minint] a validé le référencement du [participant] car les processus organisationnels du [participant]
  sont en accord avec les processus du projet 2D-Doc
- *suspended* : le [Minint] a décidé de suspendre temporairement le [participant] car les processus organisationnels ne sont pas en accord avec les processus du projet 2D-Doc, ce statut est utilisé pendant le temps nécessaire à la mise en place de mesures correctives.
- *revoked* : le [Minint] a décidé de ne plus référencer ce [participant] suite au non-respect des processus organisationnels.

Cette liste comporte l'identifiant SIRET/SIREN tel que défini dans le standard [REF DGME], la raison sociale et le statut
(cf. Annexe : Annuaire des [Participant]s par le [MinInt].)

3.3.3. Mise à disposition et disponibilité

Cette liste est disponible sur le site de l'ANTS : https://www.ants.interieur.gouv.fr.

Nota : cette information n'est pas utilisée durant le processus de vérification des signatures. Elle n'est utile que pour une
AC référencée pour vérifier que le [participant] qui s'adresse à elle est effectivement référencé.

3.3.4. Processus de référencement des [participant]s par les AC

Le processus de référencement des [participant]s est à la charge des Autorités de Certification. Une autorité de certification ne peut émettre un certificat de type « 2D-Doc » de production qu'à une entité validée comme [Participant] par le [MinInt].

3.3.4.1. Pour le gabarit des certificats des [participant]s

Le DN du champ « subject » qui identifie le [Participant] comporte :

- les attributs CountryName (C), Organization (O) et OrganizationUnit (OU) conformément au RGS et cohérents avec le numéro SIREN/SIRET du [Participant], conformément au document [REF DGME],
- un attribut commonName (CN) qui contient l'identifiant sur quatre caractères du certificat du [Participant] contenu dans le code à barres 2D, cet attribut est du type 2D-DocId :N° d'identification. Une autorité de certification n'émet qu'un seul certificat pour un CN donné.

Le champ « Subject Public Key Info » contient l'identifiant de l'algorithme à utiliser et les paramètres associés pour vérifier le code à barres de type « 2D-Doc ». Cet identifiant indique l'algorithme asymétrique à utiliser ex : ECDSA.

Comme seule la taille de la clé est disponible dans ce champ, alors la taille de clé est automatiquement associée à la fonction de hachage correspondante : NISTP256 avec SHA-256, NISTP384 avec SHA-384 et NISTP521 avec SHA-512. L'algorithme de calcul du condensat est spécifié en fonction de la courbe utilisée pour générer les paires de clé (cf. tableau ci-dessous). Cette correspondance permet de déduire l'algorithme de calcul de condensat utilisé en fonction de la taille de la clé publique fournie dans le certificat au moment de la vérification.

Courbes elliptique	Taille de la signature	Algorithme de calcul de condensat
NISTP-256	64 octets	SHA-256
NISTP-384	96 octets	SHA-384
NISTP-521	132 octets	SHA-512

Pour les aspects concernant le gabarit du certificat, l'outil doit être conforme au RFC 5280 de l'IETF. Pour les aspects concernant les performances cryptographiques, l'outil doit être conforme aux recommandations quant au choix des algorithmes du RGS.

3.3.4.2. Pour l'annuaire des certificats

Chaque AC maintient un annuaire des certificats du type « cachet serveur » émis pour chaque [participant].

3.3.5. Mise à disposition et disponibilité

Cet annuaire est disponible à l'adresse définie dans la TSL des [AC] signée par l'ANTS.

Les mises à jour et la disponibilité de cet annuaire respectent les mêmes règles que les CRLs pour le RGS niveau « * ».

4. Annexe: Liste des « Participants » par le [MinInt]

Sur le serveur web, le fichier est présenté de manière à être facilement compréhensible par un être humain. En interne, l'ANTS utilise un format XML, conforme à un schéma XSD, décrit ci-dessous.

Afin d'être facilement compréhensible par un être humain, ce fichier est transformé au moyen d'un fichier XSL.

Schéma xsd

```
<?xml version="1.0" encoding="utf-8" ?>
- <xs:schema id="NewSchema" xmlns:xs="http://www.w3.org/2001/XMLSchema">
- <xs:simpleType name="Status_Type">
- <xs:restriction>
  <xs:enumeration value="InAccord" />
  <xs:enumeration value="Suspended" />
  <xs:enumeration value="Revoked"  />
    </xs:restriction>
    </xs:simpleType>
- <xs:simpleType name="SIREN_TYPE">
- <xs:restriction base="xs:integer">
  <xs:length value="9" />
    </xs:restriction>
    </xs:simpleType>
- <xs:simpleType name="SIRET_TYPE">
- <xs:restriction base="xs:integer">
  <xs:length value="14" />
    </xs:restriction>
    </xs:simpleType>
  <xs:element name="SIREN" type="SIREN_TYPE"  />
  <xs:element name="SIRET" type="SIRET_TYPE"  />
- <xs:complexType name="Entreprise">
- <xs:choice>
  <xs:element name="SIRET" type="SIRET" />
  <xs:element name="SIREN" type="SIREN" />
    </xs:choice>
```

```
<xs:attribute name="Nom" type="xs:token" />
<xs:attribute name="Status" type="Status_Type" />
  </xs:complexType>
- <xs:element name="Liste des entreprises">
- <xs:complexType name="Liste">
- <xs:sequence>
<xs:element minOccurs="0" maxOccurs="unbounded" name="Entreprise" type="Entreprise" />
  </xs:sequence>
  </xs:complexType>
  </xs:element>
  </xs:schema>
```

Pour certains éléments, les travaux de l'INSEE sont utilisés :

- Pour le type SIREN :

```
<xs:simpleType name="SIRENType">
            <xs:restriction base="ie:ChaineNumeriqueType">
              <xs:length value="9"/>
            </xs:restriction>
          </xs:simpleType>
```

- La définition de l'élément SIREN est la suivante :

```
          <xs:element name="SIREN"
                      type="ie:SIRENType"/>
```

- Pour le type SIRET :

```
<xs:simpleType name="SIRETType">
            <xs:restriction base="ie:ChaineNumeriqueType">
              <xs:length value="14"/>
            </xs:restriction>
          </xs:simpleType>
```

- La définition de l'élément SIRET est la suivante :

```
<xs:element name="SIRET"
                      type="ie:SIRETType"/>
```