**République Tunisienne**

Ministère des Technologies de la Communication
et de l'Economie Numérique


# PROCESSUS « TN CEV 2D-Doc »

| Version | Date | Statut | Actions |
|---|---|---|---|
| 1.0 | 23/02/2017 | Validé | Création du document |

# Table des Matières

# Fonds documentaire

- **[TN CEV 2D-Doc Processus] :** Présent document. Ce document décrit les processus fonctionnels du projet, les apports nécessaires des autres documents, précise les spécifications techniques ne nécessitant pas un document spécifique.
- **[TN CEV 2D-Doc Gouvernance] :** décrit les mécanismes organisationnels et juridiques.
- **[Spec CAB 2D-Doc] :** référentiel élaboré et publié par l'ANTS de France décrivant les caractéristiques techniques des codes à barres de type 2D-Doc (voir http://www.tuntrust.tn/fr/solutions/qrsign).

En partenariat avec l'ANTS de France et l'Association Internationale de Gouvernance du Cachet Electronique Visible AIGCEV, L'Agence nationale de certification électronique TUNTRUST met en place la solution « TN CEV 2D-Doc » pour sécuriser les données échangées sous forme papier ou électronique entre l'usager et l'administration.

Le standard « TN CEV 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 « TN CEV 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 « TN CEV 2D-Doc » peut être découpé en étapes fonctionnelles simples :

- **Etape 1** : un participant émet un Cachet Electronique Visible de type « TN CEV 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 « TN CEV 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 [TN CEV 2D-Doc] :

- **[TUNTRUST]** : L'agence nationale de certification électronique, représentée par son Directeur Général ou un de ses membres qu'il désigne pour agir en son nom est chargée de la coordination du dispositif, de la mise en place des relations avec les Participants, fixe les normes techniques et la liste des documents sécurisés, valide les applications, assure les référencements, exerce un contrôle continu sur le respect des prescriptions techniques.
- **[Participant]** : Personne morale mettant en place une solution d'écriture de cachet électronique visible [TN CEV 2D-Doc] sur les documents qu'elle émet ;

- **[Usager]** : Personne morale ou physique qui reçoit un document comportant un Cachet Electronique Visible [TN CEV 2D-Doc] ;
- **[Utilisateur]** : Personne morale ou physique ayant fait le choix de lire les cachets de type [TN CEV 2D-Doc] pour avoir un élément d'information supplémentaire dans le cadre de la vérification de l'authenticité des documents.
- **[AC]** : Autorité de certification référencée par TUNTRUST qui dans le cadre de ce projet émet des certificats de signature du type « cachet serveur » selon les standards publiés par TUNTRUST ; 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 ou cachet électronique visible «TN CEV 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] accréditée et référencée par TUNTRUST
    - un [Editeur] référencé par TUNTRUST.
- **Etape 1.02 :** le candidat [participant] devient et reste un [participant]
- **Etape 1.03** : Le [participant] place, un code à barres de type [TN CEV 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 ou cachet électronique visible TN CEV 2D-Doc sont mises en forme ;
- le cachet 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 :** l'[utilisateur] 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] et un [Editeur] accrédités et référencés par TUNTRUST. |
|---|
| 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 TUNTRUST : [Processus TN CEV 2D-Doc]. Suite à ce processus, TUNTRUST émet une décision.<br>• Préciser le rôle des différentes entités pour ces référencements : [Document de gouvernance]<br>• Préciser le mode de diffusion de l'information : sur le site www.tuntrust.tn. TUNTRUST précise les raisons commerciales et les identifiants des entités référencées 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 TUNTRUST qui émet une décision.<br>• Préciser les conditions techniques pour rester [Participant] : lorsqu'informé d'un incident technique, TUNTRUST émet une décision suite à une étude d'évaluation ou d'investigation.<br>• Préciser les conditions juridiques et fonctionnelles : [Document de Gouvernance]. |

| **Etape 1.03 : Le [participant] met en place un code à barres de type [TN CEV 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 du cachet de type « TN CEV 2D-Doc » :<br>[*Spécifications techniques du Code à Barres 2D-Doc*]<br>(voir http://www.tuntrust.tn/fr/solutions/qrsign). |

### *2.1.2. La lecture de codes à barres*

| **Etape 3.01 : Décoder le cachet électronique visible de type « TN CEV 2D-Doc »** |
|---|
| L'[utilisateur] doit être en mesure de décoder les cachets sous forme de 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 cachets électroniques visuels : [Spécifications technique CAB 2D-Doc].<br>• L'[utilisateur] doit s'assurer de l'interopérabilité de la solution de lecture choisie |

| **Etape 3.02 : Récupérer l'adresse de l'annuaire de certificat de l'AC** |
|---|
| l'[utilisateur] récupère le certificat de l'AC, ainsi que l'adresse de son annuaire où sont publiés ses certificats. |
| **Action(s)** |
| • L'[Utilisateur] doit connaître l'adresse de l'annuaire de TUNTRUST : www.certification.tn<br>• 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: [Processus TN CEV 2D-Doc]. |

| **Etape 3.03 :** L'[Utilisateur] vérifie que ce certificat d'AC n'est pas révoqué. |
|---|

| |
|---|
| A partir des services en ligne de l'AC, l'[utilisateur] vérifie le statut du certificat. |
| **Action(s)** |
| • L'AC publie le statut du certificat dans son annuaire. |

| **Etape 3.04 : Récupérer le certificat du [Participant] correspondant à l'identifiant** |
|---|
| A partir des éléments présents dans le cachet électronique visible TN CEV 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.<br>• 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] : [Processus TN CEV 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.<br>• 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.<br>• 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 cachet 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 défini et publié par TUNTRUST. Les règles de disponibilité s'appliquent à l'ensemble du standard « TN CEV 2D-Doc » y compris les différents annuaires.<br>• Définir les bonnes pratiques pour les [utilisateur]s : document [Processus TN CEV 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 tests par TUNTRUST. |

| **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 « TN CEV 2D-Doc » |
| **Action(s)** |
| • La solution « TN CEV 2D-Doc » est basée sur un mécanisme identique à celui de la signature électronique. Les règles de responsabilité sont donc celles du cadre réglementaire tunisien Loi n° 2000-83 du 9 Août 2000, relatives aux échanges et commerce électroniques. |

## 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 cachets électroniques visibles**

| *Liste des* | *La liste référence la Conformité* | *Identifiants utilisés* | *Responsable de la liste* | *Standard de publication de la liste* | *Mise à jour* |
|---|---|---|---|---|---|
| **[AC] référencées** | Aux exigences stipulées par TUNTRUST | Certificat d'AC<br><br>Identifiant TUNTRUST<br><br>Adresse internet de l'annuaire de certificats émis par l'AC. | [TUNTRUST]<br>(où : www.tuntrust.tn) | Précisé par : [Processus TN CEV 2D-Doc] | à chaque nouvelle AC. |
| **Certificat de [Participant]** | Aux conditions de référencement des [participant]s par [TUNTRUST] | Certificat de [Participant]<br><br>Identifiant [TN CEV 2D-Doc] | [AC] référencée<br>(où : site internet de l'AC) | [selon RFC 4387]<br>Précisé par : [Processus TN CEV 2D-Doc] | à chaque nouveau certificat. |

**Annuaire consultable par les futurs [participant]s**

| *Liste des* | *La liste référence la conformité* | *Identifiants utilisés* | *Responsable de la liste* | *Standard de publication de la liste* | *Mise à jour* |
|---|---|---|---|---|---|
| **[Editeurs] référencés** | [Spec CAB 2D-Doc] | Identifiant fiscal<br><br>Raison commerciale | [TUNTRUST]<br>(où : www.tuntrust.tn) | Page Web : [Processus TN CEV 2D-Doc] | tous les 3 mois |

**Annuaire consultable par les AC référencées**

| *Liste des* | *La liste référence la conformité* | *Identifiants utilisés* | *Responsable de la liste* | *Standard de publication de la liste* | *Mise à jour* |
|---|---|---|---|---|---|
| **[Participants] référencés** | [Document de gouvernance] | Identifiant fiscal<br><br>Raison commerciale | [TUNTRUST]<br>(où : www.certification.tn) | Page Web : [Processus TN CEV 2D-Doc] | 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 TUNTRUST des [AC]

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

TUNTRUST référence les certificats d'autorité pouvant émettre des certificats destinés à signer des codes à barres de type « TN CEV 2D-Doc ».

### *3.1.1. Processus de référencement*

#### *3.1.1.1. Pour les aspects sécurité*

L'autorité de certification doit être accréditée par TUNTRUST pour émettre des certificats du type « TN CEV 2D-Doc ».

#### *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, [TUNTRUST] référence cette autorité de certification et lui délivre un identifiant TN CEV 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, [TUNTRUST] a un droit de supervision et de décision sur le référencement des autorités de certification.

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

## *3.2. Référencement des [Editeur]s par TUNTRUST*

### *3.2.1. Processus de référencement*

Pour être référencé, l'Editeur transmet à TUNTRUST dix feuilles de test comportant un code à barres de types « TN CEV 2D-Doc » pour des pseudo-participants. [TUNTRUST] vérifie leur conformité au standard et émet sa décision.

#### *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 identifiant fiscal.

#### *3.2.3. Mise à disposition et disponibilité*

Cette information est disponible sur le site de [TUNTRUST] : www.certification.tn;

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*

#### *3.3.1. Processus de référencement*

Le candidat [Participant] soumet 10 feuilles de test avec des données différentes à [TUNTRUST] qui décide conformément au processus défini par le document de gouvernance.

Techniquement, ce référencement est réalisé à l'aide de l'attribut organizationalUnitName

#### *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 TUNTRUST. Il est accessible en mode HTTPS.

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

- *accord* : [TUNTRUST] a validé le référencement du [participant] car les processus organisationnels et techniques du [participant] sont en accord avec les processus et les exigences techniques du projet TN CEV 2D-Doc

- *suspended* : [TUNTRUST] a décidé de suspendre temporairement le [participant] car les processus organisationnels et techniques ne sont pas en accord avec les processus du projet TN CEV 2D-Doc, ce statut est utilisé pendant le temps nécessaire à la mise en place de mesures correctives.

- *revoked* : [TUNTRUST] a décidé de ne plus référencer ce [participant] suite au non-respect des processus organisationnels et techniques.

Cette liste comporte l'identifiant fiscal, la raison sociale et le statut (cf. Annexe : Annuaire des [Participant]s.)

#### *3.3.3. Mise à disposition et disponibilité*

Cette liste est disponible sur le site de TUNTRUST : https://www.tuntrust.tn.

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 « TN CEV 2D-Doc » de production qu'à une entité validée comme [Participant] par le [TUNTRUST].

#### *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) cohérents avec l'identifiant fiscal du [Participant],
- 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 TN CEV 2D-Doc Id: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 « TN CEV 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 par TUNTRUST.

#### *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 sur le site de [AC] et sa mise à jour respectent les mêmes règles que les CRLs.

# 4. Annexe : Liste des « Participants »

Sur le serveur web de TUNTRUST, le fichier est présenté de manière à être facilement compréhensible par un être humain.