ROYAUME DU MAROC
MINISTERE DE L'EQUIPEMENT,
DU TRANSPORT ET DE LA
LOGISTIQUE

المملكة المغربية
وزارة التجهيز والنقل
واللوجستيك

N°2.2.2.1..AIR/DSA/DAC/2014

Rabat, le..18..DEC..2014

CIRCULAIRE
RELATIVE A L'UTILISATION DE LA SIGNATURE ELECTRONIQUE ET DE SYSTEMES D'ARCHIVAGE NUMERIQUE

1. Objet

La présente circulaire définit le cadre de référence pour l'utilisation des systèmes de signature électronique et d'archivage numérique. La présente circulaire définit aussi les critères d'acceptation pour l'utilisation de ces deux systèmes et avec comme document de référence la circulaire FAA AC 120-78 en sa dernière version.

2. Terminologie

Authentification : Ensemble des moyens utilisés pour valider l'identité d'un utilisateur, un mot de passe, le code PIN, le Badge ou la clé cryptographique peuvent être des moyens d'authentification.

Matériel informatique : Regroupe l'ordinateur ainsi que tous les périphériques utilisés pour le transfert de données.

Application informatique : Regroupe tous les scripts, lignes de commandes et programmes nécessaires pour le fonctionnement du matériel informatique

Signature digitale : Ensemble de données cryptées générés pour identifier le signataire du document et garantissant l'intégrité de ce dernier : La technologie des signatures digitales est le fondement d'un ensemble de produits de sécurité et de commerce électronique. Cette

technologie est basée sur la cryptographie à clé publique / privée, les infrastructures à clé publique (PKI), les réseaux privés virtuels (VPN), et sur les signatures digitales électroniques. Elle est basée aussi sur la technologie de signature digitale utilisée dans la messagerie sécurisée, ainsi que sur les standards du Web pour les transactions sécurisées.

Signature électronique : Il s'agit de l'équivalent numérique d'une signature manuscrite. La signature électronique est un son, symbole ou processus électronique attaché ou associé logiquement à un contrat ou à un autre document, qui est exécutée ou adoptée par un individu. Elle permet d'identifier et d'authentifier les individus qui introduisent, vérifient ou auditent les enregistrements informatiques. Une signature électronique combine les fonctionnalités cryptographiques offertes par les signatures digitales avec la copie d'une signature manuscrite ou toute autre marque visible acceptable dans le cadre d'un processus de signatures traditionnel. La signature électronique authentifie les données via un algorithme de hachage, et ce dans le but de fournir une authentification des utilisateurs permanente et sécurisée.

Système d'archivage électronique : Système sur lequel des données ou des manuels peuvent être renseignés, stockés et accessibles par un système informatique.

Signature : Toute forme d'identification qui permet de relier l'utilisateur à l'entrée réalisée. Elle peut être manuscrite où faisant partie d'un système de signature électronique

3. Critères pour les systèmes de signature électronique

La signature manuscrite dispose de qualités et attributs qui permettent de garantir son authenticité. L'objet des systèmes de signature électronique est de couvrir ces attributs. Les systèmes de signature peuvent se présenter sur plusieurs formes :

- Une signature digitale ;
- Une copie numérique d'une signature manuscrite ;
- Un code électronique ;
- Toute autre forme d'identification individuelle qui peut être utilisée pour l'authentification d'un enregistrement, une entrée ou document.

La signature électronique doit faire partie d'un système d'information robuste. Ce système doit au minimum couvrir les attributs suivants :

3.1 Unicité

La signature électronique doit avoir les mêmes attributs que la signature manuscrite qui garantissent son unicité. Une signature doit permettre l'identification d'un utilisateur et doit être difficilement reproductible. Une signature unique doit prouver qu'un individu est d'accord avec une communication écrite. Un des moyens pour prouver l'unicité de la signature, est l'utilisation d'une procédure d'authentification qui valide l'identité du signataire.

Un utilisateur d'un système de signature électronique doit pouvoir s'identifier. L'authenticité de cette identification doit être validée par le système de signature électronique. L'utilisation de codes constitue un exemple d'identification. Ces codes peuvent être codés dans des badges, cartes électroniques, clés cryptographiques ou tout autre moyen acceptable par l'autorité. Les systèmes utilisant des codes PIN ou des mots de passe garantissent aussi l'unicité de la signature. D'autres systèmes acceptables par l'autorité utilisant des caractéristiques physiques comme les empreintes ou signature vocales peuvent être utilisés comme moyens d'authentification.

3.2 Clarté

L'utilisateur de signature électronique doit effectuer une action délibérée et reconnaissable pour apposer sa signature. Ci-dessous des exemples de systèmes d'authentification clairs :

- Badge ;
- Signature d'un document électronique avec un stylet ;
- Appuyer sur des touches spécifiques d'un clavier ;
- Utilisation d'une signature digitale.

3.3 Périmètre

Les champs d'informations attestées par la signature électronique doivent être clairement identifiables par le signataire et les personnes consultant à posteriori l'enregistrement, l'entrée ou le document. Pour identifier le champ d'informations attestées, la signature manuscrite est positionnée à proximité dudit champ. Toutefois l'identification du périmètre attesté par signature électronique peut être réalisée en surlignant, en changeant le contraste des informations, en utilisant des bordures ou en utilisant des caractères clignotants. De plus le

système de signature doit notifier l'utilisateur que la signature est apposée. L'utilisateur doit pouvoir retrouver toutes les informations qu'il a attestées par le système de signature électronique.

3.4 Sécurité

Le niveau de sécurité quant à une signature manuscrite réside dans la difficulté de reproduire la signature par un autre individu. Le niveau de sécurité pour la signature électronique doit être équivalent à celui de la signature manuscrite. Le système de signature électronique doit empêcher un individu d'utiliser la signature d'autres personnes pour des enregistrements, entrées ou documents. De ce fait :

- Une politique et une structure doivent être mises en place pour supporter le matériel et les applications informatiques produisant la signature ;
- Le système d'authentification doit pouvoir déterminer si la signature est authentique et que l'utilisateur dispose des droits pour attester des données. Ceci peut être réalisé en comparant la signature entrée et une archive de clés. Cet attribut doit faire partie intégrante de l'application informatique ;
- Un système d'archivage doit faire partie du système de signature électronique, ceci pour stocker de manière sure les documents signés électroniquement ;
- Le système de signature électronique doit empêcher l'utilisation d'une signature appartenant à un utilisateur ayant changé de fonction/ quitté son poste. Une procédure doit être mise en place pour désactiver cette signature dès réception de la notification de changement de fonction/ démission ;
- Des procédures doivent être mises en place pour permettre la correction de documents erronés préalablement signés. Chaque mise à jour d'un document signé doit rendre la signature déjà établie caduc. Une autre signature est requise dans ce cas et doit référer aux modifications apportées au document.

3.5 Désaveu

Une signature électronique doit empêcher un signataire de nier sa signature passée sur un document. Plus la signature est difficile à reproduire plus le signataire ne pourra nier les signatures passées. Le niveau de sécurité exposé ci-dessus participe à la difficulté pour reproduire les signatures.

3.6 Traçabilité

Le système de signature électronique doit permettre de relier chaque document signé à l'individu qui l'a signé.

4. Constitution d'un dossier pour l'utilisation de signature électronique

Le dossier pour l'utilisation de la signature électronique doit contenir les éléments suivants :

- **Lettre d'intention**

Les opérateurs doivent faire parvenir à la DAC une lettre d'intention pour l'utilisation de signature électronique. Cette lettre doit décrire le système proposé ainsi que la révision apportée sur les manuels de l'opérateur ;

- **Descriptif du système de signature électronique**

Le descriptif doit expliquer comment le système de signature électronique est utilisé pendant les activités opérationnelles et de maintenance. La révision des manuels de l'opérateur doit spécifier le responsable pour l'implémentation, la mise à jour et l'audit du programme de signature électronique. La révision doit contenir aussi une description du mode de transmission des documents signés électroniquement.

4.1 Validation de la DAC

La DAC évaluera le dossier pour l'utilisation de la signature électronique, si le programme et le matériel utilisés pour la signature électronique répond aux exigences de la présente circulaire, une autorisation est accordée à l'opérateur pour l'utilisation du système de signature électronique.

5. Critères pour les systèmes d'archivage numérique

Les éléments suivants doivent être couverts par le système d'archivage numérique, elles doivent aussi être consultables par tout utilisateur autorisé du système.

5.1 Sécurité

Afin d'assurer un niveau de sécurité acceptable par l'autorité :

- Le système d'archivage numérique doit restreindre l'accès aux données confidentielles ;
- Le système d'archivage numérique doit empêcher la modification des informations archivées par le personnel non autorisé ;

- Une politique et une structure doivent être mises en place pour supporter le matériel et les applications informatiques produisant la signature.

5.2 procédures

Les procédures suivantes doivent faire partie des manuels de l'opérateur :

Accès de la DAC aux archives numérisées

Des procédures doivent être mises en place pour permettre l'accès de la DAC aux archives numérisées. L'opérateur doit désigner une personne pour assister la DAC à accéder aux archives numérisées.

Interdiction de duplication des procédures d'attribution de données

Les procédures d'attribution de données d'identification doivent empêcher leur duplication, à ce titre des procédures d'audit doivent être mise en place pour vérifier l'intégrité du programme informatique tous les 60 jours. Les rapports d'audits doivent être archivés toute en respectant les exigences réglementaires en matière d'archivage des enregistrements.

Des procédures d'audit doivent être mises en place pour vérifier l'intégrité des postes de travail utilisés pour le système d'archivage.

Transmission des archives aux clients

Afin d'assurer l'intégrité des documents lors de leur transfère aux clients des procédures doivent définir comment les archives numériques doivent être transmises à un client ou un opérateur dans le respect des réglementations DAC en vigueur. La transmission peut être soit numérique ou par papier.

Des procédures doivent être mises en places pour que le format des données « électronique ou papier » transférées puisse être exploité par le nouvel opérateur/ propriétaire d'un avion.

Mode opératoire

Afin d'assurer une utilisation souple et harmonisée de la part de la totalité du personnel autorisé des procédures doivent définir les modes opératoires pour le personnel autorisé pour l'utilisation de la signature électronique et l'accès aux archives numériques.

Programme de formation

L'exploitant doit établir et maintenir à jour un programme de formation nécessaire à l'utilisation du système. Ce programme doit être décrit dans la manuel formation de l'exploitant et comporter les prérequis nécessaires pour l'utilisation du matériel et du programme informatique.

6 Constitution d'un dossier pour l'utilisation d'un système d'archivage numérique

Lettre d'intention

Les opérateurs doivent transmettre à la DAC une lettre d'intention pour l'utilisation d'un système d'archivage numérique. Cette lettre doit décrire le système proposé ainsi que la révision apportée sur les manuels de l'opérateur.

6.1 Descriptif du système d'archivage numérique

Le descriptif doit expliquer comment le système d'archivage numérique est utilisé pendant les activités d'exploitation et de maintenance. La révision des manuels de l'opérateur doit spécifier le responsable pour l'implémentation, la mise à jour et l'audit du programme d'archivage numérique.

6.2 Validation par la DAC

La DAC évaluera le dossier pour l'archivage numérique. Si le programme les procédures et le matériel utilisés pour l'archivage numérique répondent aux exigences de la présente circulaire, une autorisation sera délivrée à l'opérateur pour l'utilisation du système de l'archivage numérique.

6. Date d'effet :

La présente circulaire prend effet à la date de sa signature.

Le Directeur de l'Aéronautique Civile

Signé .....

Le Directeur de l'Aéronautique Civile

ABDENNEBI MANAR