TSPD, IPS et CESU

Collecte Activité / Fraude / Evolutions sécurité &

Auto évaluation sécurité

IEOM

Notice de remplissage

Table des matières

Table des matières

1 Assujettissement à la collecte TSPD, IPS et CESU de l'IEOM : « Activité, Fraude et Evolutions sécurité » et « Auto évaluation des objectifs de sécurité »

1.1 Définition des termes

Les termes ci-dessous utilisés dans le document ont la signification suivante :

Émetteur	Acteur habilité à émettre des TSPD, IPS et/ou CESU, soumis réglementairement à la remise d'un rapport, sous forme de questionnaire, à l'IEOM. Il est déclarant et, selon les cas, le remettant pour la présente collecte.
TSPD	Titre Spécial de Paiement Dématérialisé
IPS	Instrument de Paiement Spécifique
CESU	Chèque Emploi Service Universel préfinancé

1.2 Contexte réglementaire

Constituée de deux volets, la collecte TSPD, IPS et CESU de l'IEOM est assurée par l'Institut d'Emission d'Outre-Mer (IEOM) au titre de la surveillance des titres spéciaux de paiement dématérialisés (TSPD), des instruments de paiement spécifiques (IPS) et des chèques emploi-service universels préfinancés émis sur support papier ou sous forme dématérialisée (CESU) émis dans les collectivités françaises du Pacifique – Nouvelle-Calédonie, Polynésie française et les îles Wallis-et-Futuna.

Les TSPD sont identifiés par Arrêté des 17 juin 2013 et 2 février 2022 fixant la liste des titres spéciaux de paiement dématérialisés en application de l'article L. 525-4-2 du code monétaire et financier. L'article 2 de l'Arrêté du 2 février 2022 le rend applicable dans les Collectivités françaises du Pacifique (en application des articles L. 773-25 en Nouvelle-Calédonie, L. 774-25 en Polynésie française et L. 775-19 dans les îles de Wallis-et-Futuna).

Les IPS sont identifiés par Arrêté des 4 juin 2018 et 2 février 2022 (publié parallèlement à celui concernant les TSPD) fixant la liste des instruments de paiement spécifiques en application de l'article L. 521-3-2 du code monétaire et financier (en application des articles L. 773-21 en Nouvelle-Calédonie, L. 774-21 en Polynésie française et L. 775-15 dans les îles de Wallis-et-Futuna).

Le chèque emploi-service universel préfinancé est un titre spécial de paiement mentionné au B de l'article L1271-1 du code du travail (Article Lp. 125-10 du Code du travail de Nouvelle-Calédonie et Articles Lp. 1234-1 à Lp 1234-14 du code du travail de Polynésie française). Selon l'article D1271-7 du code du travail (articles R. 125-1 et s. en Nouvelle-Calédonie et pas de disposition réglementaire en Polynésie française), le titre spécial de paiement mentionné au B de l'article L1271-1 est émis sur support papier ou sous forme dématérialisée, conformément aux dispositions de l'article D.1271-4. Selon la forme qu'il prend, le CESU est un TSPD ou un IPS.

La surveillance de la sécurité des différents processus de traitement de ces titres et instruments s'appuie sur les dispositions suivantes :

- Articles R 1271-22 et R1271-23 du Code du travail et L525-4-2 du Code monétaire et financier pour les TSPD-CESU, décliné dans le livre VII du CMF ;
- Article L521-3-2 du Code monétaire et financier pour les IPS, décliné dans le livre VII du CMF.

1.3 Emetteurs de Titres spéciaux de paiement dématérialisés, Instruments de paiement spécifique et chèques emploi-service universels préfinancés assujettis à la collecte

Selon la nature des titres émis, les entreprises assujetties à la collecte TSPD, IPS et CESU de l'IEOM sont celles qui émettent des titres ou instruments de ce type et les proposent à leurs clients.

Par type, sont concernés par la collecte, les émetteurs de titres ou instruments listés ci- après

Titres Spéciaux de Paiement Dématérialisés :

L'article L. 525-4-2 renvoie à un arrêté le soin de fixer la liste des titres spéciaux de paiement dématérialisés (TSPD). Il s'agit de l'arrêté du 17 juin 2013, complété par un arrêté du 2 février 2022 étendu dans les COM (article 2), qui vise :

- le titre-restaurant ;
- le chèque-repas du bénévole ;
- le titre-repas du volontaire ;
- le chèque emploi-service universel préfinancé ;
- le chèque d'accompagnement personnalisé ;
- le chèque-vacances ;
- le chèque-culture ayant pour objet exclusif de faciliter l'accès de leurs bénéficiaires à des activités ou prestations de nature culturelle et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale ;
- les titres-cadeaux et bons d'achat servis par les comités d'entreprise ou les entreprises en l'absence de comité d'entreprise, à l'occasion de certains événements personnels ou familiaux et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale et qui sont utilisables exclusivement pour l'acquisition de biens ou de services à l'intérieur d'un réseau limité de partenaires directement liés contractuellement à un émetteur de titres spéciaux de paiement, ou pour acquérir un éventail limité de biens ou de services auprès de partenaires ;
- les titres-cadeaux octroyés dans le cadre d'opérations de stimulation et de promotion des ventes et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale et qui sont utilisables exclusivement pour l'acquisition de biens ou de services à l'intérieur d'un réseau limité de partenaires directement liés contractuellement à un émetteur de titres spéciaux de paiement, ou pour acquérir un éventail limité de biens ou de services auprès de partenaires ;
- le titre-mobilité.

Instruments de Paiement Spécifique :

L'article L. 521-3-2 renvoie à un arrêté le soin de fixer la liste des instruments de paiement spécifique (IPS). Il s'agit de l'arrêté du 4 juin 2018, étendu dans les COM par un autre arrêté du 2 février 2022 qui vise :

- le titre-restaurant ;
- le chèque-repas du bénévole ;
- le titre-repas du volontaire ;
- le chèque emploi-service universel préfinancé ;

- le chèque d'accompagnement personnalisé ;
- le chèque-vacances ;
- le chèque-culture ayant pour objet exclusif de faciliter l'accès de leurs bénéficiaires à des activités ou prestations de nature culturelle et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale ;
- les titres-cadeaux et bons d'achat servis par les comités sociaux et économiques ou les entreprises en l'absence de comité social et économique, à l'occasion de certains événements personnels ou familiaux et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale et qui sont utilisables conformément aux dispositions de l'article L. 521-3-2 ;
- les titres-cadeaux octroyés dans le cadre d'opérations de stimulation et de promotion des ventes et bénéficiant à ce titre d'un régime d'exonération de cotisations et contributions de sécurité sociale et qui sont utilisables conformément aux dispositions de l'article L. 521-3-2 ;
- Le titre-mobilité.

Chèques Emploi Service Universel préfinancés :

Le chèque emploi service universel préfinancé (CESU) est un titre spécial de paiement mentionné au B de l'article L. 1271-1 du code du travail (Article Lp. 125-10 du Code du travail de Nouvelle-Calédonie et Articles Lp. 1234-1 à Lp. 1234-14 du code du travail de Polynésie française). Selon l'article D. 1271-7 du code du travail (articles R. 125-1 et s. en Nouvelle-Calédonie et il n'existe pas de disposition réglementaire en Polynésie française), le titre spécial de paiement mentionné au B de l'article L. 1271-1 du code du travail est émis sur support papier ou sous forme dématérialisée, conformément aux dispositions de l'article D. 1271-4.

C'est l'entreprise émettrice de TSPD, IPS ou titres CESU qui déclare les stocks et flux de paiement réalisés par les instruments ou titres qu'elle émet. Si cette entreprise confie le traitement de ses opérations à un autre établissement, notamment dans le cas des titres dématérialisés, elle doit avoir connaissance des modalités de traitement de ses opérations pour être en mesure de répondre correctement aux différentes rubriques du présent questionnaire. Le cas échéant, elle se fait communiquer les informations nécessaires par le prestataire qui prend en charge le traitement de ses opérations. À défaut de données réelles, elle devra fournir des données estimées et en faire état dans les parties du questionnaire permettant de commenter les réponses apportées, en précisant la méthode d'estimation utilisée.

1.4 Contacts, modalité technique de transmission de la déclaration et calendrier de la collecte TSPD, IPS et CESU de l'IEOM

La fréquence de remise diffère selon les volets de la collecte :

- Volet quantitatif de la collecte : la déclaration Statistiques, Fraude et Evolution de la sécurité est établie sur une base annuelle. La collecte débute en février et s'achève le dernier jour ouvrable d'avril.

- Volet qualitatif de la collecte : l'auto-évaluation de la sécurité des titres ou instruments est à remettre une fois tous les trois ans du 1er jour ouvrable de février au dernier jour ouvrable d'avril. Un établissement qui démarrerait ses activités sur l'année N sera tenu de remettre une première auto-évaluation à l'occasion de la collecte de l'année N+1.

La remise de l'auto évaluation de la sécurité des titres ou instruments ne concerne pas les établissements ayant déjà remis ce document au titre de l'exercice 2022 (campagne de collecte 2023).

Afin d'assurer la sécurisation de sa transmission à l'IEOM, le courrier électronique portant les fichiers déclaratifs peut être adressé à l'un des deux membres de l'équipe de surveillance (en charge des moyens de paiement scripturaux) et être chiffré et signé. La méthodologie retenue par l'IEOM repose sur le recours à l'outil S/MIME - Secure/Multipurpose Internet Mail Extensions- qui est une technologie utilisée pour sécuriser les communications par courrier électronique.

Afin de préciser la modalité de chiffrage et de signature retenue par l'IEOM, un manuel utilisateur de S/MIME est adressé à chaque correspondant identifié, agissant dans le cadre de cette collecte pour le compte d'un déclarant, émetteur de TSPD, IPS ou CESU.

Pour toute information, vous pouvez contacter les services de l'Institut d'émission d'Outre-mer à partir des coordonnées suivantes :

L'agence de l'IEOM de votre Collectivité (PMSB@ieom.nc ; PMSB@ieom.pf) ou les services du siège (IEOM-Paris-SEF-surveillance@iedom-ieom.fr)	Pour les questions portant sur la gestion opérationnelle de la collecte
sylvie.pipponiau@iedom-ieom.fr ou olivier.basseto@iedom-ieom.fr	Destinataires des courriers électroniques de réponse à la collecte
IEOM-Paris-SEF-surveillance@iedom-ieom.fr	Pour les questions d'ordre méthodologique pour lesquelles le présent guide de remplissage n'apporte pas de réponse

2 Description de la collecte TSPD, IPS et CESU de l'IEOM :

Le cadre de la collecte TSPD, IPS et CESU mis en place par l'IEOM évolue à compter de l'année 2024 (données 2023). Entre le déclarant et le siège de l'IEOM, la transmission des fichiers déclaratifs s'opère toujours par envoi d'un courrier électronique, portant en pièces jointes les tableaux renseignés, Afin d'assurer la sécurisation de la transmission, ce message peut dorénavant être chiffré et signé en recourant à l'outil S/MIME. Le protocole de chiffrage et de signature des courriers électroniques impose de n'adresser le message de réponse qu'à un unique destinataire (sylvie.pipponiau@iedom-ieom.fr ou olivier.basseto@iedom-ieom.fr).

Après renseignement des différents tableaux de données, les déclarants doivent transmettre pour l'exercice 2023 par courrier électronique, éventuellement chiffré et signé par S/Mime, adressé à l'un des deux membres de l'équipe en charge de la surveillance des moyens de paiement scripturaux du siège de l'IEOM, comprenant en PJ de leur message de réponse, le fichier suivant qui devra être renommé en conséquence :

- Volet quantitatif : **NOM**_**ENTREPRISE**_TSPD_IPS_CESU_IEOM_Stat_Activite_Fraude_Evol_securite_2023.xlsx ;

2.1 Volet quantitatif de la collecte et Renseignement du fichier relatif à l'activité, la fraude subie et à l'évolution du dispositif de sécurité de l'entreprise : « NOM_ENTREPRISE_TSPD_IPS_CESU_IEOM_Stat_Activite_Fraude_Evol_securite_2023.xlsx »

Les informations rapportées dans les deux premiers onglets, activité et fraude, sont exclusivement de nature quantitative.

Les informations rapportées dans le troisième volet sont de nature qualitative, et visent à rappeler synthétiquement les évolutions ayant eu un impact sur les objectifs de sécurité de l'émetteur au cours de l'année sous revue. Les 11 axes d'analyse renvoient aux thématiques développés dans le reporting d'auto-évaluation (cf. supra § 2.2. Volet qualitatif).

Les trois tableaux, ou onglets, du fichier Excel listent l'ensemble des TSPD, IPS et CESU que les déclarants sont susceptibles d'émettre pour le compte de leurs clients. Aussi, le déclarant doit limiter sa remise aux seuls colonnes d'instruments ou titres pour lesquels il est émetteur.
Dans une logique de renseignement par colonne (i.e. par instrument ou par titre), le renseignement des tableaux du document doit respecter les règles suivantes :

- Seules les cellules bleues doivent être renseignées ;
- Les zones grisées ne sont pas à compléter ;
- Pour chacune des lignes, les caractéristiques des champs sont précisées en « fin de ligne » dans le fichier Excel (numérique –E(X), nombre entier de longueur maximale de X chiffres-, alphanumérique –AN(X), suite de caractères alpha numériques de longueur X, …)
- Vérifier pour chacun des titres, les égalités suivantes :
    - Ligne 2.1. : Dans chaque colonne, contrôle de somme avec les lignes suivantes : 2.1. = 2.1.1 + 2.1.2 (digital) ou 2.1 = 2.1.3 (papier) ;
    - Ligne 2.2. : Dans chaque colonne, contrôle de somme avec les lignes suivantes: 2.2. = 2.2.1 + 2.2.2 (digital) ou 2.2= 2.2.3 (papier).

2.1.1. Onglet « Activité »

Les informations rapportées dans la colonne « Définition » précisent les attendus de l'IEOM en termes de renseignement des différentes cellules du tableau de l'onglet « Activité ».

N° ligne	Intitulé	Définition	Caractéristique (Papier ou Digital)	Format des champs
	Nom commercial du titre			AN (50)
	Nature juridique (TSPD, IPS, CESU)			Liste : TSPD, IPS ou CESU
	Format (Digital ou papier)			Liste : Digital ou Papier
1.	Activité d'émission période sous revue			
1.1.	Activité d'émission dans l'année			
1.1.1.	Nombre de financeurs	Nombre de clients directs de l'émetteur (CSE, employeurs, …).		E (10)
1.1.2.	Nombre de bénéficiaires	Nombre de bénéficiaires finaux des titres, utilisateurs des titres pour payer des B&S, distribués par les financeurs.		E (7)
1.1.3.	Nombre de titres papier émis dans l'année	Nombre de titres papier distribués durant l'exercice sous revue aux financeurs.	Papier	E (10)
1.1.4.	Nombre de supports physiques ou électroniques émis dans l'année pour le compte des clients.	Nombre de supports physiques ou électroniques distribués, auprès des clients, ou émis pour leur compte durant l'exercice sous revue.	Digital	E (10)
1.1.5.	Valeur des titres émis dans l'année (en XPF)	Valeur totale des titres distribués pendant l'exercice sous revue aux financeurs.	Papier et Digital	E (15)
1.2.	Titres en circulation en fin d'année			

1.2.1.	Nombre de titres papier valides en circulation	Nombre de titres papier, émis pendant l'exercice ou antérieurement, toujours valides et jamais présentés au paiement.	Papier	E (10)
1.2.2.	Nombre de supports physiques ou électroniques valides en circulation au 31/12	Nombre de supports physiques ou électroniques distribués aux financeurs et toujours actifs au terme de l'exercice sous revue.	Digital	E (10)
1.2.3.	Valeurs des titres valides en circulation au 31/12 (en XPF)	Valeur totale des titres émis pendant l'exercice, ou antérieurement, toujours valides, et jamais présentés au paiement.	Papier ou Digital	E (15)
2.	Utilisation dans l'année			
2.1.	Nombre de paiements réalisés	Nombre de transactions réalisées par utilisation d'un IPS / TSPD durant l'exercice sous revue. Par exemple, un même support (digital) utilisé 12 fois au cours de l'année devra être comptabilisé 12 fois sur ce critère	Papier ou Digital	E (10)
2.1.1.	*dont nombre de paiements à un terminal*	Nombre de transactions réalisées sur un terminal par utilisation d'un IPS /TSPD durant l'exercice sous revue.	Digital	E (10)
2.1.2.	*dont nombre de paiements à distance*	Nombre de transactions réalisées à distance par utilisation d'un IPS / TSPD durant l'exercice sous revue.	Digital	E (10)
2.1.3.	*dont nombre de paiements en titre papier*	Nombre de transactions réalisées par utilisation d'un titre en papier durant l'exercice.	Papier	E (10)
2.2.	Montant des paiements réalisés (en XPF)	Montant des transactions réalisées par utilisation d'un IPS / TSPD durant l'exercice sous revue.	Papier ou Digital	E (15)
2.2.1.	*dont montant des paiements à un terminal (en XPF)*	Montant des transactions réalisées sur un terminal par utilisation d'un IPS /TSPD durant l'exercice sous revue.	Digital	E (15)
2.2.2.	*dont montant des paiements à distance (en XPF)*	Montant des transactions réalisées à distance par utilisation d'un IPS / TSPD durant l'exercice sous revue.	Digital	E (15)
2.2.3.	*dont montant des paiements en titre papier (en XPF)*	Montant total des transactions réalisés par utilisation d'un titre en papier durant l'exercice.	Papier	E (15)
2.3.	Nombre d'accepteurs	Nombre de commerçants ou d'entreprises acceptant le paiement par utilisation d'IPS / TSPD au 31/12/N-1	Papier ou Digital	E (7)

E(X) : nombre entier d'un nombre de caractères inférieur ou égal à X.

2.1.2. Onglet « Fraude »

Les informations rapportées dans la colonne « Définition » précisent les attendus de l'IEOM en termes de renseignement des différentes cellules du tableau de l'onglet « Fraude ».

N° ligne	Intitulé	Définition	Caractéristique (Papier ou Digital)	Format des champs
	Nom commercial du titre			AN (50)
	Nature juridique (TSPD, IPS, CESU)			Renseigner TSPD, IPS ou CESU

	Format (Digital ou papier)			Renseigner Digital ou Papier
1.	Fraude enregistrée dans l'année			
1.1.	Tentatives de fraude en nombre de transactions	Renseigner le nombre de tentatives de fraude, y compris celles sans impact financier, subies par l'émetteur au cours de l'année sous revue. Doivent être comptabilisées les opérations fraudées et les tentatives de fraude ayant échouées initiées au cours de l'année sous revue		E(5)
1.2.	Tentatives de fraude en montant (en XPF)	Renseigner le montant financier associé au nombre de tentatives de fraude dénombrées à la question précédente subies par l'émetteur		E(15)
1.3.	Fraude brute en nombre de transactions	Renseigner le nombre de fraudes brutes supportées par l'émetteur, c'est-à-dire le nombre de fraudes qui n'ont pu être bloquées en dépit du dispositif de maitrise des risques en place		E(10)
1.4.	Fraude brute en montant (en XPF)	Renseigner le montant des fraudes brutes supportées par l'émetteur, c'est-à-dire le nombre de fraudes qui n'ont pu être bloquées en dépit du dispositif de maitrise des risques en place		E(15)
1.5.	Description des tentatives et des cas de fraude rencontrés (nature / canal / support…)	Description synthétique des tentatives et cas de fraude supportés par l'émetteur au cours de l'exercice sous revue.		AN [500 ; 2000]
1.6.	Nombre de supports/titres mis en opposition	Nombre de supports et / ou titres mis en opposition au cours de l'année sous revue.		AN [500 ; 2000]

E(X) : nombre entier d'un nombre de caractères inférieur ou égal à X.
AN (500-2000) : Texte en caractères alpha numériques d'une longueur comprise entre 500 et 2000 caractères.

2.1.3 Onglet « Evolution sécurité »

Les informations rapportées dans la colonne « Définition » précisent les attendus de l'IEOM en termes de renseignement des différentes cellules du tableau de l'onglet « Evolution sécurité ».

En tant que de besoin, l'examen de la situation de l'émetteur par rapport aux critères constitutifs des considérations clés de l'autoévaluation de la sécurité (cf. point 2.2.) constitue un guide utile pour la rédaction des commentaires synthétiques afférents à l'évolution du dispositif de sécurité sur les 11 thèmes abordés.

	Nom commercial du titre			AN (50)
	Nature juridique (TSPD, IPS, CESU)			Liste : TSPD, IPS ou CESU
	Format (Digital ou papier)			Liste : Digital ou Papier
1.	Évolutions ayant eu un impact sur les objectifs de sécurité			
1.1.	Gouvernance et organisation	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères,	Papier ou Digital	AN [500 ; 2000]

		précisant les évolutions apportées depuis la dernière remise en termes de gouvernance et d'organisation.		
1.2.	Évaluation des risques	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière d'évaluation des risques : expositions, système d'information, …	Papier ou Digital	AN [500 ; 2000]
1.3.	Gestion des incidents et reporting	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées en matière de gestion de tout type d'incident et d'élaboration des reportings depuis la dernière remise.	Papier ou Digital	AN [500 ; 2000]
1.4.	Contrôle et encadrement des risques	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière d'encadrement des risques (financiers, opérationnels, …).	Papier ou Digital	AN [500 ; 2000]
1.5.	Traçabilité / piste d'audit	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière de traçabilité des opérations et d'élaboration des pistes d'audit.	Papier ou Digital	AN [500 ; 2000]
1.6.	Sécurité physique du titre	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière de sécurité physique des titres émis	Papier	AN [500 ; 2000]
1.7.	Enrôlement des utilisateurs et sécurité des opérations sensibles	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière d'enrôlement des utilisateurs et des mesures de sécurité appliquées sur les opérations sensibles	Papier ou Digital	AN [500 ; 2000]
1.8.	Sécurité de la transmission des supports de titres	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise sur la sécurité entourant la transmission aux clients des supports	Papier	AN [500 ; 2000]
1.9.	Dispositif de surveillance des opérations	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise s'agissant du dispositif encadrant la surveillance des opérations initiées avec un TSPD/IPS	Papier ou Digital	AN [500 ; 2000]
1.10.	Protection des données sensibles de paiement	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise en matière de protection des données sensibles de paiement	Papier ou Digital	AN [500 ; 2000]
1.11.	Sensibilisation de l'utilisateur aux règles de sécurité	Commentaire synthétique, d'une longueur comprise entre 500 et 2.000 caractères, précisant les évolutions apportées depuis la dernière remise concernant les actions de sensibilisation des utilisateurs aux règles de sécurité liées à l'usage des TSPD/IPS	Papier ou Digital	AN [500 ; 2000]

2.2. Volet qualitatif de la collecte et Renseignement du fichier relatif à l'auto évaluation de la sécurité de l'émetteur : « NOM_ENTREPRISE_TSPD_IPS_CESU_IEOM_Auto_evaluation_securite_2023.docx »

Cette remise ne concerne pas les établissements ayant déjà remis ce document au titre de l'exercice 2022 (collecte 2023).

Les règles de renseignement du tableau « Auto évaluation de la sécurité » sont les suivantes :

- Les onze thématiques de l'auto évaluation de la sécurité de l'émetteur (Gouvernance et organisation, Evaluation des risques, gestion des incidents et reporting, Contrôle et limitation des risques, Traçabilité / piste d'audit, Sécurité physique du titre papier (IPS ou CESU), Enrôlement des utilisateurs et sécurité des opérations sensibles, Sécurité de la transmission des supports de TSPD/IPS, Dispositif de surveillance des opérations, Protection des données sensibles de paiement et Sensibilisation de l'utilisateur aux règles de sécurité) se déclinent en différentes Considérations Clés.

- Par Considération Clés, les données ***niveau de conformité*** sont à renseigner selon le nombre de critères [listés de a) à h)] associés à la Considération Clé examinée qui sont respectés. La règle d'attribution de la note de la Considération Clé, selon le nombre de critères respectés, est la suivante :

    - Note 4 - Satisfaction à l'ensemble des critères de la Considération Clé
    - Note 3 - Satisfaction à la majeure partie des critères ; non satisfaction à au moins l'un des critères
    - Note 2 - Satisfaction à la majeure partie des critères ; non satisfaction à au moins deux des critères
    - N1 - Non satisfaction de trois critères ou plus

- Le point 6 du formulaire d'autoévaluation de la sécurité, ne concerne que les émetteurs de titres ou instruments « papier ». Aussi, les émetteurs de titres dématérialisés renseigneront les cellules concernées par cette partie de l'autoévaluation avec la mention « NNCP » - Ne nous concerne pas.

- Sur les différentes lignes concernées, la couleur rouge, dans les colonnes « Niveau de sécurité » et « Références internes / commentaires », rappelle que les cellules ou champs sont à renseigner.

	AUTO-EVALUATION DE LA SECURITE DES TITRES SPECIAUX DE PAIEMENT DEMATERIALISES ET INSTRUMENTS DE PAIEMENTS SPECIFIQUES (y compris CESU)	NIVEAU DE CONFORMITE	REFERENCES INTERNES / COMMENTAIRES Obligatoire
1	**Gouvernance et organisation**		
1.1	**La politique de sécurité est formalisée et validée par une instance dirigeante de l'assujetti. Elle fait l'objet d'une mise à jour sur une base annuelle. Elle doit comporter des objectifs de sécurité clairement définis, une identification des risques sécuritaires pesant sur l'activité, une évaluation de leur sévérité et des mesures d'encadrement du risque adéquates.**		
	L'émetteur de TSPD/IPS :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum -
	a) dispose d'une politique de sécurité formalisée relative à l'émission et la gestion de TSPD/IPS comprenant notamment :		

	o une définition de la sécurité (physique et logique) du système d'information, son périmètre et ses objectifs (et notamment, la disponibilité, l'intégrité et la confidentialité du SI) o une échelle permettant la qualification du niveau de risque ; o des objectifs de sécurité définis par type de données comprenant les mesures de contrôle et les critères d'évaluation du niveau de sécurité ;		2 000 caractères alphanumériques maximum
	b) fait valider la politique de sécurité par l'instance dirigeante, qui nomme un responsable chargé de son application et de sa révision périodique au regard des risques identifiés ;		
	c) s'assure de la connaissance des règles de sécurité par tous les intervenants de la chaîne d'émission (salariés, intérimaires, prestataires….).		
1.2	**La politique de sécurité prévoit une fonction indépendante de gestion des risques et définit les rôles et responsabilités des acteurs du contrôle permanent et périodique de son application.**		
	L'émetteur de TSPD/IPS : a) dispose d'une fonction indépendante de contrôle permanent et alloue les moyens nécessaires à l'exercice du contrôle ;	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) dispose d'une fonction de contrôle périodique et se charge de veiller au respect des procédures et au caractère approprié des dispositifs de contrôle permanent. Lorsque la taille de l'entreprise ne justifie pas de confier les responsabilités du contrôle permanent et du contrôle périodique à des personnes différentes, ces responsabilités peuvent être confiées soit à une seule personne, soit à l'organe exécutif qui assure, sous le contrôle de l'organe délibérant, la coordination de tous les dispositifs qui concourent à l'exercice de cette mission;		
	c) dispose d'une charte de la fonction d'audit formalisée par la direction générale encadrant les conditions de réalisation des missions de contrôle ;		
	d) dispose d'une procédure pour les missions de contrôle qui précise notamment qu'elles donnent lieu à l'établissement de rapports remis à la direction générale et qui font l'objet d'un plan d'action par les directions opérationnelles ;		
	e) s'assure que le responsable de la sécurité n'exerce pas d'activité opérationnelle au sein de l'entreprise.		
2.	**Évaluation des risques**		
2.1	**Les émetteurs doivent conduire et documenter une évaluation de l'ensemble des risques associés à la sécurité des TSPD/IPS et relatifs tant à leur émission qu'à leur gestion ou leur acceptation. Cette évaluation doit notamment prendre en considération les risques liés au i) système informatique d'émission des TSPD/IPS (algorithmes de génération de codes, système d'autorisations, etc.) ; ii) aux éventuelles prestations externalisées (fabricants de supports carte, opérateurs télécom, développement applicatifs, réseau d'acceptation, etc.) ; iii) à l'environnement technique mis à la disposition des tiers bénéficiaires, financeurs, accepteurs impliqués (extranets, portail web, applications mobiles, etc.).**		
	L'émetteur de TSPD/IPS :		

	a) a constitué une cartographie des risques couvrant l'intégralité du périmètre des activités d'émission et de gestion des TSPD/IPS, en tenant compte notamment des risques liés au i) système informatique d'émission des TSPD/IPS (par exemple : algorithmes de génération de codes, système d'autorisations, etc.); ii) aux éventuelles prestations externalisées (par exemple : fabricants de supports carte, opérateurs télécom, développement applicatifs, réseau d'acceptation, etc.); iii) à l'environnement technique mis à la disposition des tiers bénéficiaires, financeurs, accepteurs impliqués (par exemple : extranets, portail web, applications mobiles, etc.) ;	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) veille à ce qu'une révision annuelle de l'analyse des risques, prenant en considération les nouvelles menaces et nouvelles vulnérabilités ainsi que les évolutions du système d'information ou des processus, soit validée par une instance dirigeante adéquate ;		
	c) intègre dans son évaluation les risques inhérents au recours à l'externalisation de fonctions du processus d'émission des TSPD/IPS le cas échéant ;		
	d) s'assure que les procédures d'évaluation des risques prennent en considération les résultats des audits, des inspections et des incidents identifiés ;		
	e) s'assure que la qualification du personnel chargé de l'évaluation des risques est adéquate à la fonction.		
2.2	**L'émetteur doit avoir identifié les données sensibles de paiement. Les données sensibles de paiement sont celles qui, conservées et réutilisées, permettent de réaliser des opérations frauduleuses de paiement. Elles comprennent les données permettant l'initiation d'un ordre de paiement, données d'identification, ainsi que tout autre donnée ou paramètre qui lorsque modifié frauduleusement, compromet l'intégrité et la validité d'une opération de paiement. L'évaluation des risques doit prendre en considération la nécessité de protéger et sécuriser ces données.**		
	L'émetteur de TSPD/IPS :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) met en place des procédures appropriées pour identifier les données sensibles de paiement, qui peuvent varier selon la nature du support de l'instrument de paiement utilisé (par exemple par le PAN d'une carte de paiement ou numéro de téléphone d'un utilisateur) ;		
	b) s'assure que la liste de ces données sensibles est mise à jour dans le cadre des projets d'évolutions et lorsque de nouveaux types de fraudes sont identifiés ;		
	c) prévoit les dispositifs techniques et organisationnels permettant de garantir l'authenticité, l'intégrité et la confidentialité des données sensibles de paiement.		
2.3	**Les émetteurs doivent entreprendre une revue des scénarios de risques majeurs pouvant affecter le service avant toute modification substantielle d'infrastructure ou de processus fonctionnel, ou lorsque de nouvelles menaces ont été identifiées lors d'une révision de l'analyse des risques. Cette révision générale de l'analyse des risques majeurs doit être réalisée a minima une fois par an.**		
	L'émetteur de TSPD/IPS :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) définit les risques majeurs liés à la sécurité des TSPD/IPS. Ceux-ci résultent généralement de l'indisponibilité du système d'information, des ressources humaines ou des locaux de l'entreprise ;		
	b) s'assure que la révision de l'analyse des risques majeurs fait l'objet d'une rubrique dédiée dans le cadre de la révision annuelle de l'analyse des risques.		

2.4	**Les émetteurs exercent une activité de veille qui leur permet d'adapter les protections dont bénéficient leurs titres physiques ou dématérialisés en fonction de l'évolution des techniques de fraude, afin que ceux-ci conservent toujours un niveau de sécurité adapté.**		
	L'émetteur de TSPD/IPS :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) exerce une activité de veille concernant l'évolution des méthodes de falsification et de contrefaçon des TSPD/IPS.		
	b) exerce une activité de veille concernant l'évolution des méthodes d'attaque en particulier des attaques réalisées sur les environnements d'accès distants proposés aux tiers avec lesquels il est en relation.		
	c) tient compte des informations recueillies par son activité de veille pour adapter le niveau de sécurité de ses TSPD/IPS, de ses bases de données et de ses accès réseaux.		
3.	**Gestion des incidents et reporting**		
3.1	**Les émetteurs doivent disposer d'un processus permettant de traiter, suivre et gérer les incidents de sécurité. Un tableau de bord de synthèse doit être régulièrement remis aux instances dirigeantes.**		
	L'émetteur de TSPD/IPS s'assure :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) Que les procédures d'enregistrement et de remontée des incidents de sécurité sont correctement documentées avec notamment la classification des niveaux de criticité des incidents et la liste à jour des intervenants ;		
	b) De la fiabilité du processus de remontée, d'enregistrement et de pilotage des incidents de sécurité ;		
	c) De la mise en œuvre de plans d'actions correctifs ;		
	d) De la transmission périodique aux instances dirigeantes d'un tableau de suivi des incidents et de la mise en œuvre des plans d'actions correctifs.		
3.2	**Une procédure doit être en place permettant de rapporter un incident à la Banque de France lors de la détection d'un incident de sécurité majeur lié à la gestion des TSPD/IPS.**		
	L'émetteur s'assure que la procédure de remontée des incidents de sécurité majeurs à la Banque de France est documentée avec notamment la liste à jour des intervenants et contacts.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
3.3	**L'émetteur dispose de procédures adaptées à la gestion des types d'incidents identifiés et d'un plan de secours pour les activités de traitement du TSPD/IPS. Ce plan prévoit notamment le périmètre et les modalités de sauvegarde des données, les modalités techniques et organisationnelles du passage en secours, les conditions du fonctionnement (mode normal ou dégradé), les réacheminements éventuels de flux physiques ou logiques et le retour au fonctionnement nominal. En cas de recours à une prestation externalisée, le plan de secours doit prendre en compte la capacité du prestataire à fournir le service rendu.**		
3.3.1.	L'émetteur dispose d'une procédure de gestion des sauvegardes de données. Il s'assure en particulier :		
	a) De la définition du périmètre des sauvegardes et de la nature des données concernées (par exemple: applications, données, codes sources, paramétrages, etc.)	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum -

	b) Du type de sauvegarde adéquat en fonction de la quantité et de la nature des données concernées. Le type de sauvegarde doit préciser la fréquence (par exemple: duplication en temps réel, quotidienne, hebdomadaire, etc.), la méthode de sauvegarde utilisée (par exemple: synchrone, différentielle, incrémentielle, etc.) ainsi que la localisation et le type de support employé (par exemple: bandes magnétiques externalisées, etc.) ;		2 000 caractères alphanumériques maximum
	c) Que les procédures de sauvegarde et les modalités de conservation des données sauvegardées doivent garantir le même niveau de sécurité (intégrité et confidentialité) que pour les données de production;		
	d) Que les volumes et les durées de sauvegarde doivent être suivis afin d'anticiper les limites en termes de capacité et, le cas échéant, de faire évoluer les moyens de sauvegarde ;		
	e) Que la procédure de sauvegarde doit être revue et testée à chaque modification du système d'information (nouvelles applications, mises en production, etc.).		
3.3.2.	L'émetteur dispose d'un plan de continuité des activités formalisé et testé permettant une reprise des activités selon une stratégie prédéfinie en fonction des scénarios de sinistres identifiés. L'émetteur de TSPD/IPS s'assure à ce titre :		
	a) de l'identification des scénarios de sinistres majeurs auxquels l'émetteur peut se retrouver confronté (à minima : indisponibilité du SI, indisponibilité des locaux et indisponibilité des ressources humaines) ;	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) de la définition pour chaque processus sensible de leur criticité au travers notamment de la Durée d'Indisponibilité Maximale Admissible (DIMA) et de la Perte de Donnée Maximale Admissible (PDMA) ;		
	c) de la reprise des objectifs du Plan de Continuité d'Activité (PCA) dans les contrats avec ses prestataires ;		
	d) de la disponibilité des moyens, en particulier techniques, logistiques et humains, qui sont nécessaires à leur continuité ;		
	e) de l'existence d'un site de repli : celui-ci doit être accessible et disponible dans un délai compatible avec les besoins de reprise des activités, et sa localisation doit assurer un profil de risque différent du site principal ;		
	f) de la mise en place d'une cellule de crise chargée de coordonner la mise en œuvre du plan de continuité ;		
	g) des exercices de secours doivent être régulièrement réalisés ;		
	h) que le PCA fait l'objet d'un Maintien en Conditions Opérationnelles (MCO) afin d'évaluer son efficacité, sa cohérence vis-à-vis des exigences des métiers, et de s'assurer que tous les intervenants ont connaissance de leurs rôles. Le MCO doit notamment permettre de vérifier que les informations sont disponibles et à jour, les moyens de communication sont opérationnels et que les prises de décision peuvent s'opérer.		
4.	**Contrôle et limitation des risques**		
4.1	**Lors de la conception et de l'exploitation des services liés aux TSPD/IPS, les émetteurs doivent disposer d'un système d'information permettant une séparation des environnements (développement, test et production).**		
	L'émetteur a mis en œuvre une séparation des environnements (études, test, production) relatifs au système de gestion des TSPD/IPS.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
4.2	**Une procédure de gestion des habilitations doit être formalisée, actant notamment le principe du minimum de privilèges acquis par défaut et définissant la politique d'accès aux environnements logiques et physiques sur tout le cycle de vie (attribution, modification, suppression).**		

	a) L'émetteur s'assure que chaque utilisateur du système d'information (salariés, prestataires, intérimaires, etc.…) doit être reconnu par un identifiant unique et personnel.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) Chacun des utilisateurs du système d'information est référencé dans un annuaire central d'habilitations. Les habilitations sont attribuées et régulièrement mises à jour conformément à une procédure de gestion des habilitations et systématiquement soumises à validation hiérarchique.		
4.3	**Les émetteurs doivent disposer de solutions appropriées permettant de protéger les infrastructures de communication (réseau, intranet, serveurs, etc.) contre les tentatives d'attaques.**		
	L'émission de TSPD/IPS requiert l'utilisation d'un système de gestion informatisé des titres dématérialisés, lequel devant être protégé contre les tentatives d'attaque:	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) sur les infrastructures réseau de l'émetteur : celui-ci doit veiller à la correcte installation et maintenance des équipements réseau ;		
	b) sur les applications en veillant à installer les mises à jour des systèmes d'exploitation et des antivirus et à protéger les codes sources.		
4.4	**Lors de la conception des services, les émetteurs doivent veiller à ce que le minimum de données sensibles soit impliqué dans chacun des processus fonctionnels.**		
	L'Émetteur de TSPD/IPS s'assure que les données sensibles ne sont pas utilisées inutilement dans un processus afin de préserver leur intégrité et confidentialité.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
4.5	**Les mesures de sécurité mises en place pour réaliser la transaction de paiement doivent être testées par l'entité en charge des fonctions de contrôle afin de valider leur robustesse et leur efficacité. Toute modification de ces mesures doit être validée dans un processus planifié, formalisé et documenté.**		
	L'Émetteur de TSPD/IPS doit s'assurer que les mesures de sécurité mises en place :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) sont bien intégrées au périmètre du responsable de la sécurité des systèmes d'information ;		
	b) ont bien été testées quant à leur robustesse et efficacité ;		
	c) font régulièrement l'objet d'une procédure de mise à jour.		
4.6	**Les mesures de sécurité mises en œuvre sur les TSPD/IPS doivent faire l'objet d'un contrôle périodique afin de garantir leur robustesse et pertinence. Ces audits doivent être réalisés par des entités indépendantes (interne ou externe) des fonctions opérationnelles à une fréquence définie au regard de l'importance des risques encourus.**		
	L'Émetteur de TSPD/IPS doit s'assurer que :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) un contrôle périodique garantit la robustesse et la pertinence des mesures de sécurité ;		
	b) la fréquence de ces audits prend en compte les risques encourus ;		
	c) les entités en charge de ces audits sont indépendantes ;		
	d) le résultat de ces audits est communiqué aux instances dirigeantes.		

4.7	**Dans le cas où les fonctions liées à la sécurité des TSPD/IPS sont externalisées, il convient de prévoir au contrat les dispositions relatives à la conformité aux recommandations formulées dans le présent rapport.**		
	L'Émetteur doit s'assurer que les contrats avec ses prestataires prennent en compte les recommandations à mettre en œuvre. Le prestataire s'engage à respecter les recommandations et permet à l'Émetteur de vérifier la conformité de ces processus.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
5.	**Traçabilité / piste d'audit**		
5.1	**Les émetteurs doivent disposer d'un processus adéquat permettant de piloter, tracer et restreindre l'accès i) aux données sensibles de paiement ; ii) aux ressources critiques logiques et physiques (réseau, systèmes de base de données, modules de sécurité, etc.).**		
	Les traces informatiques correspondent aux enregistrements systématiques et temporaires d'informations caractéristiques des transactions opérées au sein du système d'information, issus des applications (bases de données, applications), des systèmes, des infrastructures réseaux et sécurité ou des équipements des réseaux. Le processus de gestion des traces doit permettre à l'émetteur de vérifier que les règles en matière de sécurité des SI sont correctement appliquées et que la sécurité qui doit en résulter est bien assurée.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
5.2	**Seules les personnes dûment habilitées par les émetteurs doivent être en mesure d'exploiter la piste d'audit et ce pour une durée adaptée à leur activité conformément aux règles fixées par la loi « Informatique et libertés », dont la bonne application est garantie par la Commission nationale de l'informatique et des libertés (CNIL).**		
	L'émetteur s'assure :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) du strict encadrement des rôles et responsabilités des acteurs impliqués dans la gestion des traces;		
	b) de la définition des données à journaliser et la durée de conservation de celles-ci en tenant compte de l'objectif fonctionnel poursuivi.		
6.	**Sécurité physique du titre papier (IPS ou CESU)**		
6.1	**L'émetteur s'assure de la sécurité des supports physiques du titre papier. Tout au long de la période de conservation obligatoire, la qualité, la disponibilité et l'exploitabilité technique des éléments archivés est assurée.**		
	L'émetteur s'assure de la sécurité des supports physiques du titre TSPD/IPS, il prévoit notamment de :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) fournir aux bénéficiaires et aux accepteurs l'ensemble des caractéristiques des signes de sécurité permettant d'authentifier ses titres et assure une communication large et régulière de ses informations et recommandations auprès des bénéficiaires et des accepteurs ;		
	b) disposer d'une procédure destinée à détecter la perte de qualité des archives logiques qu'il conserve. La bonne application de cette procédure fait l'objet d'une vérification régulière ;		
	c) disposer d'une procédure destinée à détecter la perte de qualité des archives physiques qu'il conserve. La bonne application de cette procédure fait l'objet d'une vérification régulière ;		
	d) disposer d'une procédure visant à s'assurer de la lisibilité dans le temps des supports archivés;		

	e) la faculté de reconstituer les informations constituant les éléments logiques (ex : fichiers d'opérations) qui auraient été altérés ou qui auraient disparu (ex : altération des supports d'archivage) ;		
	f) disposer d'une procédure visant à s'assurer de la lisibilité des reproductions destinées à l'archivage de longue durée.		
6.2	**L'émetteur dispose d'une procédure de remboursement des titres papiers prenant notamment en compte les informations relatives aux incidents de perte ou vol de titres papiers et permettant aux accepteurs de disposer préalablement de ces informations lors du remboursement d'un titre papier.**		
	L'émetteur :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) a mis en place un circuit d'alerte qui permet aux autres acteurs de déclarer que des titres papier ont été volés, perdus ou détériorés et que cela empêche leur remboursement.		
	b) dispose d'une procédure de mise en opposition des titres papier déclarés volés, perdus ou détériorés.		
	c) a mis en place une procédure permettant aux autres acteurs de savoir si un titre papier donné a été mis en opposition.		
	d) effectue une vérification régulière de la bonne application et de l'adéquation de son circuit d'alerte et de ses procédures de mise en opposition et d'information des acteurs. Il prend, le cas échéant, les mesures correctives qui apparaissent nécessaires.		
6.3	**L'émetteur s'assure qu'un titre papier ne peut être remboursé qu'une seule fois quelle que soit la modalité choisie parmi celles qui sont offertes par l'émetteur.**		
	L'émetteur :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) dispose d'une procédure éprouvée et régulièrement actualisée lui permettant de s'assurer qu'il ne rembourse un même titre qu'une seule fois, quelle que soit la forme de ce titre (papier ou dématérialisée) ;		
	b) intervient, lors d'une demande de remboursement en double, auprès de l'acteur concerné et prend toute mesure utile visant à limiter le risque de répétition de l'incident. Lors de la procédure de gestion des doubles présentations physique/dématérialisé, il s'assure du caractère effectif de la récupération, auprès du bénéficiaire, des sommes versées auprès des accepteurs.		
6.4	**Les accepteurs reçoivent des émetteurs les informations nécessaires à la reconnaissance des titres papier contrefaits, en opposition ou nuls (déjà remboursés en dématérialisés).**		
	L'émetteur :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) met à la disposition des bénéficiaires des titres papier comportant un ou plusieurs procédés destinés à protéger ceux-ci contre la falsification et la contrefaçon (ex : papier sensible au lavage et au grattage, encres réagissant à divers types d'éclairages, micro lettres, filigranes, etc.).		
	b) informe les acteurs impliqués dans le traitement des formules papier des procédés dont il a doté ses formules afin de leur permettre d'être mieux protégés contre la falsification et la contrefaçon.		

6.5	**Les environnements de production (centres de fabrication et personnalisation, plateaux informatiques, plates-formes de gestion ou d'archivage temporaire et long terme) sont situés dans des locaux bénéficiant de mesures de sécurité adaptées aux risques encourus. Le fonctionnement et l'efficacité de ces mesures sont régulièrement testés et leur accès est strictement encadré.**		
	L'émetteur :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) dispose d'un plan de sécurité physique couvrant tous les locaux affectés aux activités se rapportant aux titres papier. Ces locaux sont notamment ceux dans lesquels sont fabriqués, stockés, échangés, remboursés ou détruits les titres papier. Ce sont également ceux des plateformes de gestion qui donnent accès aux logiciels de traitement des opérations, les plateaux informatiques qui hébergent les infrastructures de réseaux ou les matériels de tri-capture, ou encore les lieux de stockage temporaire ou d'archivage long terme des actifs logiques (reproductions, données de remboursement).		
	b) prévoit, dans le plan de sécurité physique des locaux, des mesures adaptées aux risques relatifs aux biens qui y sont gérés qui couvrent au moins la protection contre l'incendie, les incidents liés à l'alimentation en fluides (eau, électricité) et la lutte contre l'intrusion et sont régulièrement testées et vérifiées.		
	c) dispose d'un mode de stockage sécurisé adapté à la protection des moyens physiques et logiques entrant dans la constitution des signes de sécurité présents dans les titres papier qu'il fabrique.		
	d) dispose de traces des accès aux locaux dans lesquels sont entreposés les biens qui apparaissent les plus sensibles au regard de son analyse de risques, afin de pouvoir les utiliser en cas d'incident.		
6.6	**L'acheminement des titres (originaux ou équivalents numérisés) lors de leur fabrication et leur mise à disposition ainsi que les transferts de flux d'informations liés à la commande ou au remboursement de titres bénéficient de mesures de protection appropriées destinées à en prévenir l'altération, le vol, ou la perte.**		
	L'émetteur :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) a analysé ses risques de perte ou de vol des titres papier, dès les premiers stades de leur fabrication, ainsi que des supports d'équivalents transportés. Cette analyse couvre l'ensemble des acheminements, notamment ceux qui sont liés aux déplacements au cours des différents stades de fabrication, à la mise à disposition, la collecte, le traitement, l'archivage et la destruction ou le transport dans le cadre des échanges physiques.		
	b) dispose de procédures d'acheminement appropriées qui permettent de répondre aux besoins de sécurité identifiés par l'analyse. Ces procédures mettent notamment en œuvre des moyens de protection, de détection d'incident et d'alerte qui répondent à la sensibilité des biens acheminés et des risques potentiels pour l'émetteur et les autres acteurs du système de paiement par titres papier si ces biens venaient à être volés ou perdus.		
	c) effectue un suivi régulier de l'adéquation et de la bonne application de ses procédures.		
	d) intervient dans les meilleurs délais lorsqu'il constate un défaut d'application des procédures établies ou lorsque celles-ci se révèlent insuffisantes ou inadéquates pour assurer le niveau de protection souhaité contre le vol ou la perte.		
7.	**Enrôlement des utilisateurs et sécurité des opérations sensibles**		

7.1	**Toute opération considérée comme sensible (en particulier les opérations d'enrôlement de l'utilisateur, de commande, de délivrance et d'opération de paiement) doit être protégée par un mécanisme d'authentification renforcée.**		
	a) Dans le cadre des opérations sensibles, l'émetteur de TSPD/IPS doit toujours s'assurer de l'identité de la personne qui effectue l'opération en utilisant un mécanisme d'authentification renforcée. Lors de l'enrôlement, pour valider les données utilisées, l'émetteur doit compléter la déclaration d'identité initiale par un mécanisme d'authentification renforcée. Il doit être indiqué au contrat qu'en cas d'échec de l'authentification renforcée, l'émetteur refuse l'exécution de l'opération.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) L'émetteur de TSPD/IPS doit s'assurer que les commerçants qui acceptent le paiement en TSPD/IPS permettent de mettre en œuvre une authentification renforcée de leurs clients pour les opérations sensibles.		
	c) L'émetteur de TSPD/IPS doit régulièrement réévaluer la pertinence de sa solution d'authentification renforcée au regard des menaces potentielles ainsi que des attaques de fraude constatées.		
	d) Dans le cas où l'émetteur n'impose pas d'authentification renforcée sur les opérations de paiement, celui-ci devra justifier son choix par une analyse des risques documentée. Cette analyse devra par exemple expliciter les mesures compensatoires mises en place par l'émetteur lui permettant de ne pas avoir recours à une authentification renforcée sur les opérations sensibles.		
	e) Lorsqu'une opération de paiement n'est pas sécurisée par une authentification renforcée, l'émetteur de TSPD/IPS doit veiller à maintenir un taux de fraude à minima équivalent à celui observé pour les paiements à authentification renforcée.		
7.2	**L'émetteur sécurise les environnements de commande de titres mis à la disposition des financeurs et sécurise le processus de délivrance des titres à ces derniers ou aux utilisateurs. En cas de compromission de l'environnement de commande du financeur, l'émetteur dispose d'une procédure de blocage des accès.**		
	a) Le processus de commande de TSPD/IPS doit être sécurisé par une authentification renforcée permettant de s'assurer que la personne est bien habilitée par le financeur pour effectuer cette opération. En cas de compromission, l'émetteur de TSPD/IPS doit être en mesure de bloquer le ou les compte(s) habilité(s) à passer des commandes de TSPD/IPS.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) Le processus de mise à disposition des TSPD/IPS pour l'utilisateur doit faire l'objet d'une procédure formalisée. En cas de remise des TSPD/IPS à un organisme tiers (financeur, comité d'entreprise, etc.), l'émetteur et l'organisme doivent avoir formalisé un accord précisant les conditions de conservation, de gestion et de distribution des TSPD/IPS.		
7.3	**L'émetteur doit limiter le nombre de tentatives de connexion et définir des règles de fin de session lorsque l'employeur ou l'utilisateur est connecté à son environnement de gestion. Lorsque le nombre maximum de tentatives de connexion est atteint, le compte de l'utilisateur doit être bloqué et une procédure doit être formalisée définissant les règles et conditions de déblocage du compte de l'utilisateur.**		
	- L'émetteur a défini et mis en œuvre un ensemble de règles d'habilitation aux environnements d'émission et de gestion des TSPD/IPS, qui régit les conditions et limitations d'accès aux services (durée maximale des sessions, nombre de tentatives de connexion, modalités de blocage/déblocage des comptes,...).	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum

7.4	**L'enrôlement et l'équipement du bénéficiaire en dispositif de paiement doivent être sécurisés et faire l'objet d'une procédure formalisée.**		
	L'émetteur de TSPD/IPS a défini et formalisé les conditions d'enrôlement et d'équipement des utilisateurs. Il veille à un niveau de sécurisation adéquat de ces deux processus permettant de s'assurer de la délivrance des TSPD/IPS à l'utilisateur final pour ce qui concerne l'enrôlement, et de la sécurisation du consentement à l'opération de paiement pour ce qui concerne l'équipement.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
8.	**Sécurité de la transmission des supports de TSPD/IPS**		
8.1	**L'émetteur a analysé ses risques de perte ou de vol des supports. Cette analyse couvre l'ensemble des transports à réaliser pour l'acheminement jusqu'à l'utilisateur final et prend donc en compte l'environnement du financeur.**		
	L'émetteur de TSPD/IPS doit analyser les risques liés à l'acheminement des supports des TSPD/IPS en prenant en compte la chaine complète, notamment l'environnement du financeur dans le cas où une partie de l'acheminement jusqu'à l'utilisateur est assuré par un organisme tiers qui lui est rattaché (services comptables du financeur, comité d'entreprise, etc…)	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
8.2	**L'émetteur dispose de procédures d'acheminement appropriées qui permettent de répondre aux besoins de sécurité identifiés par l'analyse. Ces procédures mettent notamment en œuvre des moyens de protection, de détection d'incident et d'alerte qui répondent à la sensibilité des actifs acheminés et des risques pour l'émetteur et les autres acteurs du système si ces supports venaient à être volés ou perdus.**		
	a) L'émetteur doit mettre en place des mesures de protection visant à sécuriser l'acheminement des supports des TSPD/IPS vers les utilisateurs.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) L'émetteur de TSPD/IPS assure un suivi des supports des titres délivrés pour détecter les incidents lors de l'acheminement.		
	c) La délivrance du code utilisateur personnel permettant de confirmer une opération de paiement par TSPD/IPS est réalisée distinctement de la délivrance du support physique de paiement.		
8.3	**L'émetteur effectue, au titre du contrôle interne, un suivi régulier de l'adéquation et de la bonne application de ses procédures de transmission des supports de TSPD/IPS.**		
	a) Les procédures de gestion relatives à l'émission et à la gestion des TSPD/IPS doivent être actualisées régulièrement en fonction des évolutions relatives à la politique de sécurité, aux processus opérationnels et aux systèmes d'information. Un dispositif de contrôle permanent s'assure de leur correcte application.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) L'émetteur intervient dans les meilleurs délais lorsqu'il constate un défaut d'application des procédures ou lorsque celles-ci se révèlent insuffisantes ou inadéquates pour assurer le niveau de protection souhaité contre le vol ou la perte des supports de TSPD/IPS.		
	c) L'émetteur de TSPD/IPS s'assure que les mesures de protection mises en place pour protéger l'acheminement des TSPD/IPS restent cohérentes avec les vulnérabilités et menaces identifiées.		
8.4	**L'accès du personnel aux locaux de stockage des supports est enregistré. Les enregistrements comportent l'identification des personnes ayant eu accès à ces locaux et ont pour vocation d'identifier l'origine d'un incident ayant eu le cas échéant un impact sur la sécurité.**		

	a) L'Émetteur s'assure que les sites de stockage des équipements sont munis de contrôles d'accès.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) Les données enregistrées lors des accès physiques aux locaux de stockage permettent d'identifier les personnes concernées.		
9.	**Dispositif de surveillance des opérations**		
9.1	**Les émetteurs doivent disposer d'un système de détection et prévention de la fraude. Les règles définies permettent de déceler les comportements potentiellement frauduleux sur la base d'un ensemble de critères (IP, liste noire, compteurs, etc.…).**		
	L'Émetteur de TSPD/IPS doit s'assurer :	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	a) qu'il utilise un système de prévention et de détection de la fraude efficace pour identifier les opérations suspectes avant de les autoriser ;		
	b) que son système est maintenu à jour (paramétrages, règles, etc.).		
9.2	**Le système de détection de la fraude doit être en mesure de prendre en compte toutes les fraudes et tentatives de fraude qui peuvent intervenir depuis l'émission des titres jusqu'à leur utilisation et leur remboursement final.**		
	Le système de prévention et de détection de la fraude doit prendre en compte les paramètres pertinents, (par exemple la date de la transaction, la localisation du commerçant, l'adresse IP, le montant). Dans le cas où l'émetteur ferait cohabiter titres papiers et titres dématérialisés, celui-ci s'assure notamment que le système de gestion prévoit qu'un titre ne peut être présenté deux fois au paiement ou au remboursement.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
10.	**Protection des données sensibles de paiement**		
10.1	**Toutes les données utilisées à des fins d'identification (identifiant, mot de passe, données personnelles, etc.) ainsi que les interfaces clients doivent être protégées contre l'usurpation et les accès frauduleux (par exemple en chiffrant le stockage et/ou la transmission).**		
	L'émetteur de TSPD/IPS a identifié les données sensibles et a mis en place des mesures de sécurité dédiées pour lutter contre le vol, l'accès ou la modification non autorisée de celles-ci. Ces mesures s'appliquent aussi bien au système d'information interne à l'émetteur qu'aux environnements mis à disposition pour les partenaires (financeurs, accepteurs, entreprises, etc.) et pour les utilisateurs (extranets de consultation des soldes, etc.).	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
10.2	**L'émetteur doit s'assurer de l'intégrité et de la confidentialité des données transmises entre l'accepteur et l'acquéreur par exemple par la mise en place d'une liaison chiffrée.**		
	L'émetteur de TSPD/IPS doit s'assurer que les données échangées de bout-en-bout avec l'accepteur ou l'acquéreur sont protégées par chiffrement et que leur intégrité est vérifiée.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
10.3	**L'émetteur s'assure que les dispositifs d'acceptation de leurs TSPD/IPS garantissent l'intégrité de la transaction et qu'ils sont régulièrement évalués sur leur résistance aux tentatives d'intrusion et de compromission.**		
	L'émetteur doit s'assurer du niveau de sécurité des dispositifs d'acceptation du TSPD/IPS, en particulier par :		

	a) une évaluation régulière de la robustesse des dispositifs d'acceptation aux différentes typologies de tentatives de compromission ;	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) la surveillance d'indicateurs dont le but est de détecter les comportements susceptibles d'être liés à une fraude sur le dispositif d'acceptation ;		
	c) la capacité à désactiver le parc de dispositifs d'acceptation ainsi que la faculté de déploiement rapide de mises à jour logicielle et/ou matérielle.		
10.4	**L'émetteur doit s'assurer que les accepteurs ne stockent pas de donnée sensible, ou dans le cas contraire que ces derniers ont mis en place un niveau de protection des données approprié (par exemple au moyen d'une procédure de chiffrement). En cas de non-respect de ces obligations, l'émetteur peut suspendre le contrat avec l'accepteur.**		
	a) L'émetteur de TSPD/IPS doit encourager les commerçants à ne pas stocker de données sensibles. Dans la mesure où il est légitime qu'ils puissent avoir accès à certaines de ces données a posteriori, l'émetteur de TSPD/IPS doit proposer les services adéquats pour que les commerçants n'aient pas à les stocker ou exiger contractuellement, dans le cas contraire, qu'elles soient correctement protégées.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) L'émetteur de TSPD/IPS doit s'assurer régulièrement du respect de ces bonnes pratiques par les commerçants et prendre les mesures nécessaires pour inciter le commerçant à les respecter. L'émetteur de TSPD/IPS pourra mettre fin au contrat en cas de non-conformité.		
11.	**Sensibilisation de l'utilisateur aux règles de sécurité**		
11.1	**L'émetteur doit veiller à la sensibilisation des utilisateurs aux règles de sécurité des TSPD/IPS en particulier par la mise à disposition :** **· de préconisations permettant à l'utilisateur d'utiliser les TSPD/IPS en préservant la sécurité de ses accès ;** **· de procédures à suivre en cas de perte ou vol de l'instrument de paiement délivré pour réaliser une opération de paiement en TSPD/IPS;** **· de procédures à suivre en cas de détection d'utilisation abusive ou frauduleuse.**		
	a) L'émetteur de TSPD/IPS doit mettre en place une communication claire indiquant aux utilisateurs et financeurs la manière de recevoir des TSPD/IPS, de les utiliser et la règle de sécurité à appliquer pour se prémunir contre une utilisation frauduleuse.	Choix entre 4, 3, 2 et 1	500 caractères alphanumériques minimum - 2 000 caractères alphanumériques maximum
	b) L'émetteur de TSPD/IPS doit prévoir un moyen d'informer ses utilisateurs et financeurs en cas d'incident majeur ou d'évolution du système les impactant.		
	c) L'émetteur de TSPD/IPS doit mettre à disposition de ses utilisateurs une procédure compréhensible à suivre en cas de perte ou vol de son équipement de paiement et en cas de détection d'utilisation abusive ou frauduleuse. En complément du système de détection en place (cf. 8.1), l'émetteur de TSPD/IPS doit indiquer à ses utilisateurs la manière dont ils peuvent être notifiés concernant les opérations soupçonnées d'être frauduleuses.		