



**RÉFÉRENTIEL SUR LA SÉCURITÉ DES TITRES
CHEQUES EMPLOI-SERVICE UNIVERSELS**

Février 2015

SOMMAIRE

1.	INTRODUCTION.....	3
2.	PÉRIMÈTRE.....	4
3.	MISE EN OEUVRE.....	5
4.	PRÉSENTATION DES OBJECTIFS DE SÉCURITÉ.....	6
5.	OBJECTIFS DE SÉCURITÉ.....	7
	GOVERNANCE DE LA SÉCURITÉ ET DISPOSITIFS DE CONTRÔLE.....	7
	Objectif de sécurité 1 : Gouvernance et organisation.....	7
	Objectif de sécurité 2 : Évaluation des risques.....	7
	Objectif de sécurité 3 : Gestion des incidents et reporting.....	7
	Objectif de sécurité 4 : Contrôle et encadrement des risques.....	8
	Objectif de sécurité 5 : Traçabilité / piste d'audit.....	8
	MESURES DE SÉCURITÉ SPÉCIFIQUES.....	10
	Objectif de sécurité 6 : Sécurité physique du titre CESU.....	10
	Objectif de sécurité 7 : Enrôlement des utilisateurs et sécurité des opérations sensibles ...	10
	Objectif de sécurité 8 : Sécurité de la transmission des supports de CESU.....	11
	Objectif de sécurité 9 : Dispositif de surveillance des opérations.....	11
	Objectif de sécurité 10 : Protection des données sensibles de paiement.....	11
	Objectif de sécurité 11 : Sensibilisation de l'utilisateur aux règles de sécurité.....	12
6.	GLOSSAIRE.....	13

1. INTRODUCTION

La loi n° 2013-100 du 28 janvier 2013 confie à la Banque de France la mission de s'assurer de la sécurité des titres spéciaux de paiement dématérialisés (ci-après TSPD) dont le Chèque Emploi-Service Universel préfinancé (ci-après CESU) et de la pertinence des principes de sécurité applicables en la matière.

Cette mission de surveillance des TSPD vient compléter celle déjà exercée sur le titre papier dans le code du travail (Article R1271-15), qui prévoit notamment que l'émetteur de CESU s'engage à assurer la sécurité à toutes les étapes du processus prenant en compte les objectifs de sécurité définis par la Banque de France dans le cadre de sa mission de surveillance.

La loi dispose notamment (art L 524-4 du code monétaire et financier) que les émetteurs adressent à la Banque de France un rapport annuel justifiant de la sécurité des titres spéciaux de paiement dématérialisés qu'ils émettent et gèrent.

Le présent référentiel décrit les objectifs de sécurité attendus par la Banque de France relatifs à l'émission et à la gestion des CESU, qu'ils soient émis sous forme papier ou dématérialisée. Il est complété par un guide d'évaluation qui détaille les modalités d'application de ces objectifs de sécurité et sert de support au rapport annuel adressé par les émetteurs à la Banque de France ; ce guide se substitue au précédent « Questionnaire sur la sécurité du CESU » mis en place en 2007, et sur la base duquel les émetteurs rendaient compte annuellement du niveau de sécurité atteint sur chaque objectif de sécurité.

2. PÉRIMÈTRE

Les objectifs de sécurité établis par ce référentiel s'appliquent à tout émetteur de CESU.

Les émetteurs de CESU doivent mettre en œuvre ces objectifs de sécurité définis sur la base d'une analyse des risques couvrant l'ensemble des processus liés à l'émission, la gestion et l'acceptation des CESU. Cette analyse des risques doit être régulièrement actualisée au regard des évolutions fonctionnelles ou techniques dans l'environnement des CESU.

Les objectifs de sécurité définis dans ce référentiel doivent être considérés comme un minimum requis pour la sécurité des CESU. Ceux-ci pourront cependant être révisés selon l'évolution des menaces. Ils doivent s'intégrer au dispositif général de sécurité, de gestion des incidents et de continuité de service mis en place par l'émetteur.

Les objectifs de sécurité sont formulés de façon à être indépendants des techniques et technologies employées.

Lorsqu'un émetteur de CESU externalise des prestations de service, celui-ci demeure pleinement responsable de toutes les obligations qui lui incombent, en particulier celles relatives à la sécurité des CESU. L'émetteur doit alors s'assurer que les mesures mises en place par ses prestataires et opérateurs techniques dans ce cadre sont conformes aux objectifs de sécurité énoncés dans le présent document.

Le présent référentiel est consacré exclusivement aux pratiques sécuritaires associées à l'émission, la gestion et l'acceptation des CESU ; il n'a pas notamment vocation à traiter des dispositifs de lutte contre le blanchiment et le financement du terrorisme. De la même manière, le présent référentiel n'a pas vocation à s'assurer du respect des dispositions législatives ou réglementaires spécifiques aux CESU telles que précisées dans le décret du 6 mars 2014. Les émetteurs devront se rapprocher des autorités compétentes en la matière.

3. MISE EN OEUVRE

Le référentiel présente 11 objectifs de sécurité s'appliquant aux CESU. Chaque objectif de sécurité est caractérisé par des considérations clés (CC).

La vérification du respect de la mise en œuvre de ces objectifs est assurée par la Banque de France, conformément au mandat qui lui a été confié par les articles L.525-4 du code monétaire et financier et R.1271-15 du code du travail. À cette fin, les émetteurs doivent étayer leur évaluation sur la conformité aux objectifs de sécurité par des éléments tangibles permettant à la Banque de France d'apprécier cette conformité. Dans le cas où un objectif de sécurité ne serait pas mis en œuvre, ou seulement partiellement respecté, l'émetteur devra en expliquer les raisons.

4. PRÉSENTATION DES OBJECTIFS DE SÉCURITÉ

Les objectifs de sécurité sont organisés en deux chapitres :

- 1. Gouvernance de la sécurité et dispositifs de contrôle :** dans le cadre de son dispositif de maîtrise des risques, l'assujéti doit évaluer l'adéquation des contrôles sécuritaires au regard des risques (externes et internes) associés à l'émission, à la gestion et à l'acceptation des CESU. Le premier chapitre regroupe les objectifs relatifs à la gouvernance, l'identification de ces risques et leur évaluation. Il énonce également les attentes de la Banque de France au regard du dispositif de surveillance et de son évaluation, des mesures de contrôle des risques et des mesures d'encadrement des risques.
- 2. Mesures de sécurité spécifiques :** le second chapitre expose les attentes de la Banque de France concernant la sécurité attachée aux transactions de paiements réalisés au moyen des titres spéciaux CESU (enrôlement, identification, initiation du paiement, pilotage et surveillance des transactions). Le chapitre propose en outre des objectifs relatifs à la sensibilisation des utilisateurs sur la sécurité des CESU.

5. OBJECTIFS DE SÉCURITÉ

GOVERNANCE DE LA SÉCURITÉ ET DISPOSITIFS DE CONTRÔLE

Objectif de sécurité 1 : Gouvernance et organisation

L'émetteur de CESU doit disposer d'un ensemble documentaire formalisé dans lequel sont définis les rôles et responsabilités des acteurs du système de paiement par titre CESU. L'émetteur doit par ailleurs formaliser une politique de sécurité relative à l'émission et la gestion des CESU, qui est régulièrement mise à jour.

1.1 CC Les rôles et responsabilités des acteurs du système de paiement par titre CESU sont clairement identifiés (banques centralisatrices, financeurs, centrale de règlement) au sein d'un corpus documentaire formalisé et régulièrement actualisé.

1.2 CC La politique de sécurité est documentée, validée par une instance dirigeante de l'assujéti. 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.

1.3 CC 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.

Objectif de sécurité 2 : Évaluation des risques

Les émetteurs doivent définir leur niveau de sécurité requis sur la base d'une analyse des risques liés à la sécurité des CESU.

2.1 CC Les émetteurs doivent conduire et documenter une évaluation de l'ensemble des risques associés à la sécurité des CESU et relatifs tant à leur émission qu'à leur gestion ou à leur acceptation. Cette évaluation doit notamment prendre en considération les risques liés au i) système informatique d'émission des CESU (algorithmes de génération de codes, système d'autorisations, etc.) ; ii) aux éventuelles prestations externalisées (par exemple : fabricants de supports carte, opérateurs télécom, développements applicatifs, réseau d'acceptation, etc.) ; iii) l'environnement technique mis à la disposition des tiers bénéficiaires, financeurs, accepteurs impliqués (par exemple : extranets, portail web, applications mobiles, etc.) ; iv) le champ d'application de l'habilitation (et de ses extensions) qu'a reçue l'émetteur pour émettre des CESU.

2.2 CC L'émetteur doit avoir identifié les données sensibles de paiement. Les données sensibles de paiement sont celles qui, conservées et réutilisées, permettraient de réaliser des opérations frauduleuses de paiement. Elles comprennent les données permettant l'initiation d'un ordre de paiement, les 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.

2.3 CC Les émetteurs doivent entreprendre une revue des 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 à minima une fois par an.

2.4 CC 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.

Objectif de sécurité 3 : Gestion des incidents et reporting

Les émetteurs doivent disposer d'un système de surveillance des incidents relatif à l'émission, la gestion et l'acceptation des CESU, permettant un recensement exhaustif des incidents. Les réclamations des clients doivent être comprises dans ce dispositif. Ce système de surveillance doit comprendre une procédure de

remontée des incidents qui permette une information adéquate auprès des instances dirigeantes, ainsi qu'auprès de la Banque de France sur les incidents qualifiés de majeurs (par exemple intrusions, vol de données, faille de sécurité, etc.).

3.1 CC Les émetteurs doivent disposer d'un processus permettant d'identifier, gérer et suivre les incidents de sécurité. Un tableau de bord de synthèse doit être régulièrement remis aux instances dirigeantes.

3.2 CC Une procédure doit être mise 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 CESU.

3.3 CC L'émetteur doit disposer de procédures adaptées à la gestion des types d'incidents identifiés et d'un plan de secours pour les activités de traitement du CESU. 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 a pris en compte la capacité du prestataire à fournir le service rendu.

Objectif de sécurité 4 : Contrôle et encadrement des risques

Les émetteurs doivent mettre en œuvre des mesures de sécurité, en conformité avec la politique de sécurité physique et logique, en vue d'encadrer les risques identifiés.

4.1 CC L'émetteur dispose de personnel avec des compétences et de moyens nécessaires à l'exercice des fonctions de contrôle et de gestion opérationnelle de la sécurité.

4.2 CC Lors de la conception et de l'exploitation des services liés aux CESU, les émetteurs doivent disposer d'un système d'information permettant une séparation des environnements (développement, test et production).

4.3 CC 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).

4.4 CC Les émetteurs doivent disposer de solutions appropriées permettant de protéger les infrastructures de communication (réseau, intranet, serveurs, etc.) contre les tentatives d'intrusion.

4.5 CC 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.

4.6 CC Les mesures de sécurité mises en place pour réaliser la transaction de paiement doivent être testées par le responsable de la sécurité afin de valider leur robustesse et leur efficacité. Toute modification de ces mesures doit être validée dans un processus planifié, formalisé et documenté.

4.7 CC Les mesures de sécurité mises en œuvre sur les CESU doivent faire l'objet d'un contrôle périodique afin de garantir leur robustesse et leur 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.

4.8 CC Dans le cas où les fonctions liées à la sécurité du CESU sont externalisées auprès de prestataires tiers, il convient de prévoir contractuellement les dispositions relatives à la conformité aux principes de sécurité formulés dans le présent référentiel.

Objectif de sécurité 5 : Traçabilité / piste d'audit

Les émetteurs doivent mettre en place un processus permettant l'établissement d'une piste d'audit pour chacune des transactions.

5.1 CC 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.)

5.2 CC 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.

MESURES DE SÉCURITÉ SPÉCIFIQUES

Objectif de sécurité 6 : Sécurité physique du titre CESU

L'émetteur s'assure de la sécurité des supports physiques du titre CESU. Il veille à garantir la qualité, la disponibilité et l'exploitabilité technique des éléments archivés.

6.1 CC L'émetteur s'assure de la sécurité des supports physiques du titre CESU. Tout au long de la période de conservation obligatoire, la qualité, la disponibilité et l'exploitabilité technique des éléments archivés est assurée.

6.2 CC 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 intervenants de disposer préalablement de ces informations lors du remboursement d'un titre CESU.

6.3 CC L'émetteur s'assure qu'un titre CESU ne peut être remboursé qu'une seule fois quelle que soit la modalité choisie parmi celles qui sont offertes par l'émetteur.

6.4 CC Les intervenants reçoivent des émetteurs les informations nécessaires à la reconnaissance des titres CESU contrefaits, en opposition ou nuls (déjà remboursés en dématérialisés).

6.5 CC 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.

6.6 CC 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.

Objectif de sécurité 7 : Enrôlement des utilisateurs et sécurité des opérations sensibles

L'émetteur doit formaliser une analyse des risques qui définit les opérations sensibles devant faire l'objet d'une authentification renforcée¹.

7.1 CC 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.

7.2 CC 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 doit disposer d'une procédure de blocage des accès.

7.3 CC 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.

¹ L'authentification renforcée se définit par « Un ensemble de procédures fondées sur l'utilisation d'au moins deux des trois éléments caractérisant la possession, la connaissance ou l'identité propre d'une personne :

- élément possédé par la personne (token ou jeton d'authentification, carte à puce, téléphone portable, etc.) ;
- élément connu par la personne et elle seule (mot de passe, identifiant, etc.) ;
- élément constitutif de l'identité de la personne (empreinte biométrique, etc.).

Ces trois éléments doivent être indépendants dans le sens où la compromission de l'un ne doit pas entraîner la compromission de l'autre. En outre, l'un de ces trois facteurs au moins doit être non rejouable et non reproductible (excepté pour la biométrie) ». Source : recommandations de la Banque Centrale Européenne sur la sécurisation des paiements sur internet :

<http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf>

7.4 CC L'enrôlement et l'équipement du bénéficiaire en dispositif de paiement doivent être sécurisés et faire l'objet d'une procédure formalisée.

Objectif de sécurité 8 : Sécurité de la transmission des supports de CESU

L'acheminement physique des supports CESU dématérialisés, quand ils existent², bénéficie de mesures de protection appropriées, destinées à assurer l'intégrité des supports physiques et logiques pendant leur transfert afin de prévenir et détecter les risques de perte ou de vol.

8.1 CC 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.

8.2 CC 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.

8.3 CC L'émetteur effectue, au titre du contrôle interne, un suivi régulier de l'adéquation et de la bonne application de ses procédures en matière de transmission des titres CESU.

8.4 CC 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 CESU.

8.5 CC 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.

Objectif de sécurité 9 : Dispositif de surveillance des opérations

La surveillance des transactions vise à prévenir, détecter et bloquer les tentatives de paiement suspectées d'être d'origine frauduleuse. Cette surveillance doit être encadrée par une procédure formalisée définissant les règles et typologies d'alertes.

9.1 CC 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, volumes anormaux, etc.)

9.2 CC 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.

9.3 CC L'émetteur s'assure que les dispositifs d'acceptation de ses CESU garantissent l'intégrité de la transaction et qu'ils sont régulièrement évalués sur leur résistance aux tentatives d'intrusion et de compromission.

Objectif de sécurité 10 : Protection des données sensibles de paiement

L'émetteur de CESU s'assure de la protection des données sensibles et du respect des règles de sécurité relatives à leur utilisation (création, stockage, traitement, transmission) dans les processus d'émission et d'acquisition.

10.1 CC 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).

² Par exemple dans le cas des CESU émis sur un support de type « carte de paiement »

10.2 CC 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.

10.3 CC 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.

Objectif de sécurité 11 : Sensibilisation de l'utilisateur aux règles de sécurité

Les émetteurs doivent fournir un support d'information adéquat aux utilisateurs sur les principes de sécurité relatifs à l'utilisation d'un CESU dématérialisé, ainsi que les risques associés.

11.1 CC L'émetteur doit veiller à la sensibilisation des utilisateurs aux règles de sécurité des CESU dématérialisés en particulier par la mise à disposition :

- de préconisations permettant au bénéficiaire d'utiliser les CESU papier ou dématérialisés 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 CESU dématérialisé ;
- de procédures à suivre en cas de détection d'utilisation abusive ou frauduleuse.

6. GLOSSAIRE

Les termes suivants sont définis dans le cadre du rapport:

- Accepteur : société permettant aux utilisateurs de payer des prestations au moyen des titres spéciaux de paiement.
- Acquéreur : prestataire externalisé chargé de traiter les flux d'acquisition d'ordres de paiement en TSP dématérialisés de l'émetteur.
- Émetteur : société émettrice de titres spéciaux de paiement.
- Financeur : personne morale participant au financement du CESU et le plus souvent en charge de leur distribution auprès des utilisateurs.
- Intervenant : personne morale agréée ou déclarée au titre des articles L. 7232-1 et L. 7232-1-1 du code du travail dont les prestations peuvent être payées au moyen du titre CESU.
- Utilisateur : détenteur, bénéficiaire d'un titre spécial de paiement.
- Donnée sensible : donnée d'un utilisateur ou d'un financeur permettant directement ou indirectement de
 - réaliser une commande de CESU ou une opération de paiement,
 - permettre l'identification ou l'authentification d'un utilisateur ou d'un responsable du financeur.