BANQUE DE FRANCE
EUROSYSTÈME

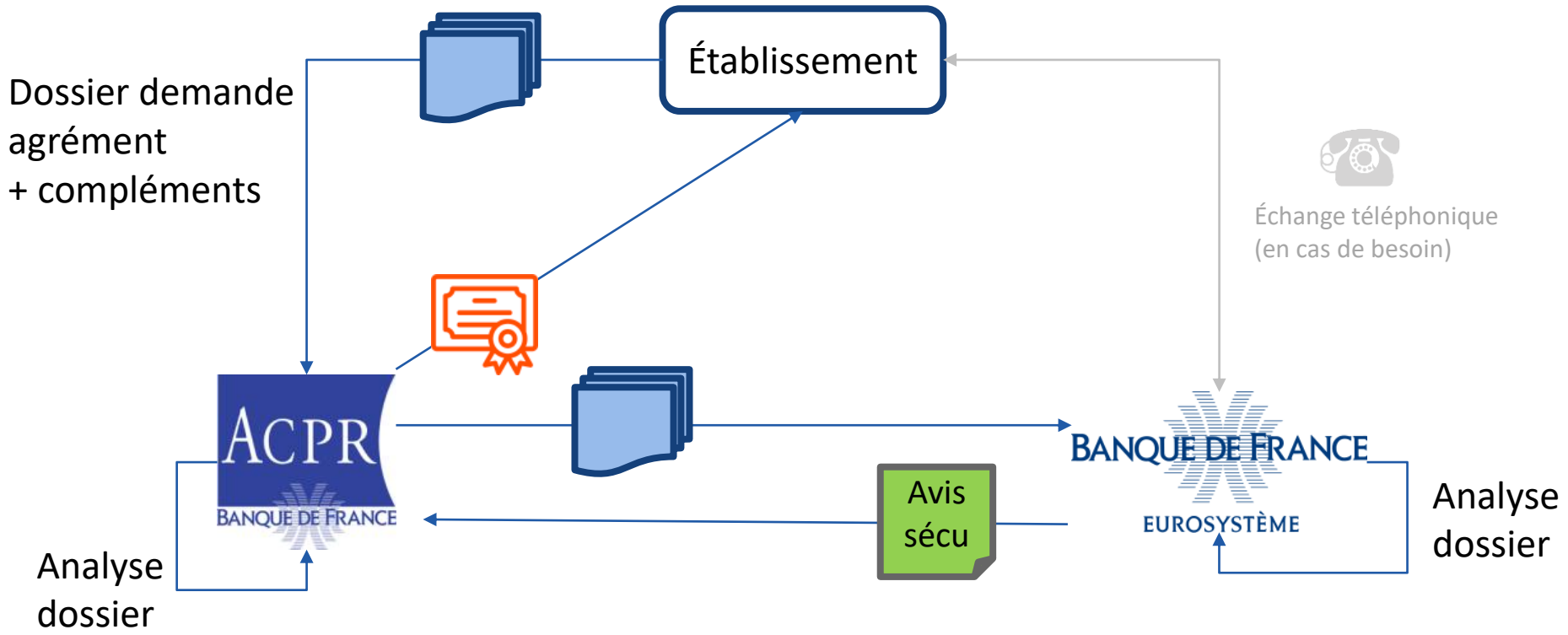
L'AVIS DE LA BANQUE DE FRANCE SUR LA SÉCURITÉ DES PAIEMENTS

PIERRE BIENVENU / TRÂN HUYNH
SMPS

12/10/2020

LA BANQUE DE FRANCE ET LA SÉCURITÉ DES PAIEMENTS

Art. L141-4 CMF : La Banque de France s'assure de la sécurité des moyens de paiement (…) et de la pertinence des normes applicables en la matière. Si elle estime qu'un de ces moyens de paiement présente des garanties de sécurité insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier.



LE CARRÉ DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

L'authentification forte du payeur

L'identification des opérations à risque

&

La sécurité physique et logique

La vigilance des utilisateurs

- **Réglementation** en matière de sécurité des moyens de paiement (DSP2 etc.)
- **Référentiels** de sécurité de l'Eurosystème et de la Banque de France
- **Recommandations** et bonnes pratiques de l'Observatoire de la Sécurité des Moyens de Paiement (OSMP)

BANQUE DE FRANCE
EUROSYSTÈME

UN AVIS DE SÉCURITÉ EN 4 TEMPS

I. COMPRENDRE L'ACTIVITÉ POUR IDENTIFIER LES RISQUES INTRINSÈQUES

II. APPRÉCIER LA QUALITÉ DE LA GOUVERNANCE EN MATIÈRE DE SÉCURITÉ DES PAIEMENTS

III. ÉVALUER LA SÉCURITE PHYSIQUE ET LOGIQUE DE L'ENVIRONNEMENT TECHNIQUE DES OPERATIONS DE PAIEMENT

IV. MESURER L'EFFICACITÉ DES DISPOSITIFS DE PREVENTION ET DE LUTTE CONTRE LA FRAUDE

I. COMPRENDRE L'ACTIVITÉ POUR IDENTIFIER LES RISQUES INTRINSÈQUES

Comprendre l'activité de l'établissement à travers les cinématiques

En soutien de l'ACPR, vérifier que les services de paiement demandés sont cohérents avec les cinématiques

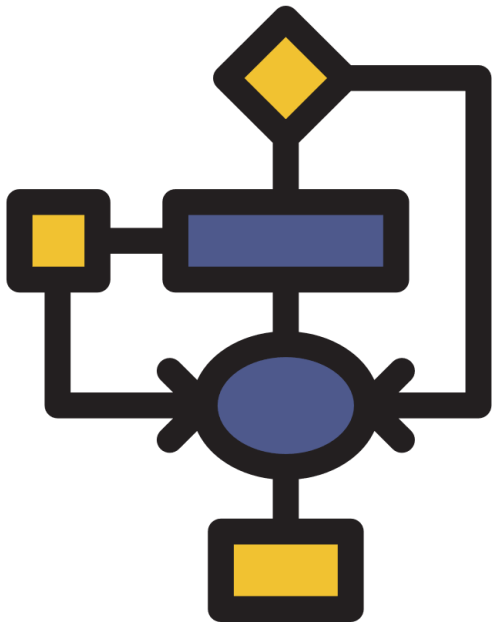
Identifier les risques intrinsèques à l'activité en s'appuyant sur notre connaissance de la fraude

II. GOUVERNANCE ET PILOTAGE DU DISPOSITIF DE SÉCURITÉ DES PAIEMENTS

La BDF vérifie:

- Une organisation claire des responsabilités et de la reddition des comptes
- Un dispositif de contrôle permanent et périodique, notamment l'application de la politique de sécurité du SI (PSSI)
- Un contrôle des prestataires de services essentiels externalisés (PSEE) et des agents
- Un dispositif de continuité d'activité (PCA ou PUPA)

II. GOUVERNANCE ET PILOTAGE DU DISPOSITIF DE SÉCURITÉ DES PAIEMENTS



BDF recherche un dispositif dynamique d'évaluation des risques:

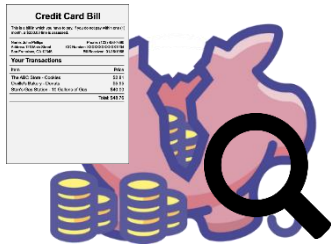
- Cartographie des risques (« *pierre angulaire* »)
- Recensement de la fraude se traduisant par des reportings internes et à destination des autorités
- Traitement réactif des incidents

II. GOUVERNANCE ET PILOTAGE DU DISPOSITIF DE SÉCURITÉ DES PAIEMENTS

BDF vérifie la mise en place de dispositifs suscitant la participation des utilisateurs à la lutte contre la fraude:

- Assistance commerciale
- Assistance en cas de fraude
- Contestation des opérations

III. SÉCURITÉ PHYSIQUE ET LOGIQUE: LES INSTRUMENTS DE PAIEMENT



* * *

Caractéristiques de l'instrument

↓

Risques techniques

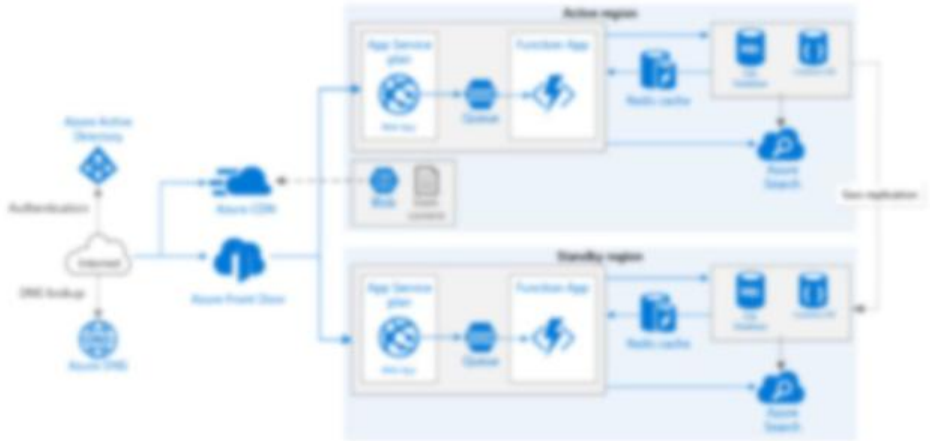
↓

Fraudes possibles

↓

BDF : renforcer les maillons techniques faibles détectés

III. SÉCURITÉ PHYSIQUE ET LOGIQUE: LE SYSTÈME D'INFORMATION (SI)



Architecture technique détaillée / Gestion des droits d'accès, des données sensibles de paiement, des sauvegardes, des certificats, des clés de chiffrements

↓

BDF : challenger l'établissement sur sa capacité à protéger les données sensibles de paiement et la robustesse du SI

FOCUS SUR LA SÉCURISATION DES DONNÉES SENSIBLES

Données sensibles sauvegardées dans le système d'information (IBAN, numéro de carte, identifiants bancaires etc.)

HSM mutualisé :

- l'administration doit être assurée par l'établissement demandeur,
- la gestion des clés est réalisée par le HSM

HSM dédié

IV. LA SÉCURITÉ DES OPÉRATIONS DE PAIEMENT ET LUTTE CONTRE LA FRAUDE

Enrôlement des clients, de leurs équipements, authentification forte du payeur

Surveillance des opérations, identification des opérations à risque et mesures complémentaires (temporisation etc.)

Action de sensibilisation auprès des utilisateurs et formation des équipes

ANNEXE

Se préparer à la surveillance permanente : déclarations à la BDF

RAPPEL DES OBLIGATIONS DE DÉCLARATIONS STATISTIQUES

Cartographie et Fraude aux moyens de paiement

- Intègre les exigences de statistiques de l'ABE et de la BCE en matière de statistiques de paiement et de fraude
- Fréquence annuelle devient semestrielle en 2021
- Via ONEGATE-OSCAMPS, remise en format XML (saisie en ligne ne sera plus possible) et identification via le LEI

Annexe au rapport de contrôle interne sur la sécurité des moyens de paiement

- Informer des changements structurants dans l'offre de moyens de paiement (produits, innovations etc.) et dans le dispositif de lutte contre la fraude
- Via ONEGATE-SURFI par le même chemin que pour le rapport de contrôle interne

RAPPEL DES OBLIGATIONS DE NOTIFICATION

Incidents majeurs

- Dispositif pour alerter la Banque de France et l'ACPR sur les incidents majeurs opérationnels et de sécurité
- Les critères sont ceux des Orientations de l'EBA de 2017 au titre de l'art. 96 DSP2 (EBA/GL/2017/10)
- Outil Sharebox à solliciter via 2323-notifications-ut@banque-france.fr

Refus de remboursement

- PSP n'effectue pas le remboursement immédiat d'une opération de paiement non autorisée au motif qu'il soupçonne une fraude de l'utilisateur
- Art. 71 DSP2 transposé art. 133-18 CMF
- Via ONEGATE-OSCAMPS

Blocage d'un PSP tiers

- PSP gestionnaire de compte bloque l'accès d'un compte de paiement en ligne qu'il gère à un PSP tiers en raison d'un accès non autorisé ou frauduleux
- Via 2323-notifications-ut@banque-france.fr