L’exemption de mécanisme d’urgence applicable aux API: présentation du formulaire ACPR

Réunion publique du 18 mars 2019

ACPR – Banque de France

Plan de la présentation

I. **Rappel des textes de référence et calendrier**

II. **La demande d'exemption:**

1. Disponibilité et performance de l'API
2. Sécurité opérationnelle de l'API

⇨ Questions bienvenues au fil de l'eau.

I. Textes de référence et calendrier

- DSP 2: Règlement délégué UE 2018/389: entrée en application au **14 septembre 2019.**

- Orientations sur la procédure d'exemption publiées par l'ABE le 4 décembre 2018 (24 janvier 2019 en français).

- Décret 2018-1228 du 24 décembre 2018 qui prévoit notamment la procédure d'exemption pour les APIs et la mise en œuvre anticipée du règlement délégué 2018/389 en France.

- Instruction n° 2019-I-01 créant le formulaire de demande d'exemption de mécanisme d'urgence applicable à une interface dédiée d'accès aux comptes tenus par un prestataire de service de paiement gestionnaire de compte: une reprise des orientations de l'Autorité Bancaire Européenne.

I. Textes de référence et calendrier

- Trois possibilités pour les prestataires de services de paiement gestionnaires de comptes (PSPGC) au 14 septembre 2019:

1. Pas d'une interface dédiée mise en œuvre : accès via le site de banque en ligne **avec authentification du tiers**:
   - pas d'autorisation ACPR

2. Interface dédiée mise en œuvre dotée d'un mécanisme de secours (accès banque en ligne avec **authentification du tiers**):
   - pas d'autorisation ACPR

3. Une API a été mise en œuvre, sans mécanisme de secours.
   - l'ACPR doit s'être prononcée favorablement sur l'octroi d'une exemption avant le 14/09/2019 sous peine de non-conformité du PSPGC.

I. Textes de référence et calendrier

- Détail du calendrier prévisionnel pour une demande d'exemption accordée au 14/09 (procédure Silence Vaut Acceptation 2 mois)

  - 14/09: date limite d'obtention d'une exemption pour les PSPGC ayant décidé la mise en œuvre d'une API.

  - 14/07: date limite de dépôt d'un dossier **complet** pour assurer un retour de l'ACPR d'ici au 14/09.

  - 14/04: date limite de mise à disposition d'une API répondant aux conditions d'**utilisation étendue** (le dossier déposé à l'ACPR ne peut sinon pas être considéré comme complet).

I. Textes de référence et calendrier

- Détail du calendrier prévisionnel pour une demande d'exemption accordée au 14/09 (procédure Silence Vaut Acceptation 2 mois)

  - 14/03 : date limite fixée par les RTS pour la mise à disposition de la documentation et de l'environnement de test de l'API**.** Néanmoins, le PSPGC devra démontrer que la mise à disposition de cet environnement à cette date a bien permis aux PSP tiers de se connecter à l'API et l'utiliser dans des conditions étendues à compter du 14/04.

  - 14/01: date recommandée par l'ACPR pour la mise à disposition par les PSPGC de la documentation liée aux API, et d'un dispositif d'essai, laissant un délai de 3 mois pour atteindre les conditions d'une utilisation étendue.

II. La demande d'exemption

1. **Qui peut demander?**
2. **Disponibilité et performance de l'API:**
   A. Niveau de service, disponibilité, performance
   B. Publication de statistiques
   C. Tests de résistance
   D. Obstacles
   E. Conception et satisfaction
   F. Utilisation étendue de l'interface
   G. Résolution des problèmes
   H. Filiales européennes
3. **Sécurité opérationnelle de l'API**

II.1 La demande d'exemption: qui?

- Tous les prestataires de services de paiement gestionnaires de comptes (PSPGC) qui offrent un service de consultation des comptes en ligne donc les EC, les EP, et les EME dès lors qu'ils offrent de tels services.

- Une exemption est nécessaire par entité juridique (code CIB).

- Dans le cadre d'un groupe ayant décidé de déployer la même API pour plusieurs entités juridiques, une demande peut être effectuée à l'aide **d'un seul formulaire**: dans ce cas, il faudra renseigner la liste exhaustive des CIB concernés dans le formulaire.

II.2 A. Disponibilité et performance de l'API

- L'objectif de cette partie est de s'assurer que les interfaces dédiées disposent de la même robustesse que celles destinées aux utilisateurs des services de paiement du PSPGC

- Des **indicateurs clés de performance** (ICP) doivent être définis, permettant de comparer l'interface dédiée et celle pour les utilisateurs directs

  - Pour le niveau de service, les ICP comprennent a minima la résolution des problèmes, l'assistance en dehors des heures de bureau, le suivi, les plans d'urgence et la maintenance

  - Ils doivent être clairement définis, et être au moins aussi exigeants que pour les interfaces destinées aux utilisateurs des services de paiement du PSPGC

II.2 A. Disponibilité et performance de l'API

- Pour la **disponibilité**, les ICP doivent couvrir a minima la **durée quotidienne de bon fonctionnement** de **toutes les interfaces** (clients et dédiée) et le **temps d'arrêt quotidien** de toutes les interfaces

- **Mode de calcul défini dans l'orientation 2.4**

- Pour la performance, les ICP sont les temps moyens par jour en millisecondes pour fournir les informations aux différentes catégories d'établissements amenés à utiliser l'API

II.2. B. Publication de statistiques

- Les PSPGC doivent publier des statistiques aisément accessibles :
  - Les statistiques en question doivent reprendre **sur une base quotidienne** les indicateurs de disponibilité et la performance.
  - Elles portent sur les interfaces dédiées et **chacune des interfaces mise à la disposition des utilisateurs de services de paiement** du PSPGC
  - Le calendrier de publication doit être communiqué accompagné d'un lien vers le lieu de la publication. Si ce dernier n'a pas encore été élaboré, la rubrique du site internet où ces statistiques seront disponibles doit être clairement indiquée
  - Les publications doivent se faire sur une base **trimestrielle**

II.2.C. Tests de résistance

- **Quatre points** à respecter au cours de ces tests pour qu'ils soient considérés comme complets:

  - « a. la capacité à supporter l'accès de plusieurs prestataires d'initiation et d'agrégation (+ services de paiement qui émettent des instruments de paiement liés à une carte?);
  - b. la capacité à gérer un nombre extrêmement élevé de demandes de la part des prestataires sur un laps de temps limité sans défaillance;
  - c. l'utilisation d'un nombre extrêmement élevé de sessions ouvertes simultanément pour des demandes d'initiation de paiement, d'information sur les comptes et de confirmation de la disponibilité des fonds; et
  - d. les demandes portant sur d'importants volumes de données. »

- Les questions du formulaire visent à vérifier quelles hypothèses ont été sélectionnées pour procéder aux tests, quels problèmes ont été identifiés, et **quelles conclusions en ont été retirées** (procédures pour les juguler et risque résiduel)

II.2.D. Obstacles

- Objectif: vérifier que les différentes étapes d'authentification ne constituent pas une **entrave** au sens du règlement 2018/389 (article 32, paragraphe 3)

- Indication de la/les différentes méthodes d'authentification possibles pour l'interface dédiée: redirection, découplage, intégration, ou combinaison de ces méthodes.

- Des captures d'écran sont demandées, reprenant les étapes de l'authentification pour 1) les interfaces pour les utilisateurs de services de paiement et 2) **pour chacune des méthodes d'authentification** pour les interfacés dédiées

  - Cette question permet de vérifier qu'il n'existe pas d'étape superflue comparativement à l'interface des utilisateurs directs; toute étape supplémentaire doit faire l'objet d'une justification

II.2. E. Conception et satisfaction

- Indiquer si l'API répond à une « **initiative de marché »**.
  - ✓ Si oui: résumé des spécifications techniques et fonctionnelles de l'interface dédiée, en justifiant leur conformité à la DSP2 et du règlement 2018/389
  - ✓ Si non: obligation pour le demandeur de remplir le questionnaire en annexe

- Fournir les éléments permettant d'attester qu'une collaboration avec les tiers a bien été initiée par le PSPGC

- Indiquer l'endroit sur le site internet du PSPGC où la mise à disposition du résumé des spécifications de l'API a été **publiée,**

- Confirmer la date du début des tests et leur conformité aux orientations de l'ABE (6.5).

- Fournir un résumé des résultats du test, comprenant notamment le nombre de prestataires ayant participé au test, les retours d'expériences faits par ceux-ci, les problèmes identifiés et les mesures prises pour y faire face.

II.2. F. Utilisation étendue de l'interface

- Rappel: une phase de **3 mois d'utilisation étendue** est impérative pour l'obtention d'une exemption. Cette période peut être comprise dans les six mois de la phase de test

- Afin de vérifier si l'utilisation a bien été étendue au cours de cette période, le nombre et la nature des utilisateurs est demandée, de même que le nombre de leurs demandes ayant fait l'objet d'une réponse

- Si peu d'intérêt d'un test par les prestataires, l'ACPR sera amenée à évaluer que des **efforts raisonnables** ont été entrepris pour que l'interface soit utilisée aussi largement que possible – notamment par la communication mise en œuvre pour informer de sa disponibilité

II.2.G. Résolution des problèmes

- L'ACPR sera amenée à évaluer le dispositif de résolution des problèmes de l'API, sous tous ses aspects: **détection, résolution, clôture**.

- Une attention particulière doit être portée aux problèmes signalés par les utilisateurs

- Les problèmes non résolus **ne doivent pas affecter le niveau de service de l'API**

II.2.H. Filiales dans l’EEE

- **L’ACPR doit être informée si une demande a été adressée pour une filiale utilisant la même API dans un autre État de l’EEE à des fins de coordination entre autorités.**

II. 3. Sécurité opérationnelle

- **Fourniture d'un rapport d'expert sur la sécurité de l'API tel que prévu au 5° de l'article D. 133-10 introduit par l'article 1er du décret n° 2018-1228 du 24 décembre 2018**

BANQUE DE FRANCE
EUROSYSTÈME

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

A.STERVINOU, T.HUYNH
SERVICE DE SURVEILLANCE
DES MOYENS DE PAIEMENT SCRIPTURAUX

18 MARS 2019

BANQUE DE FRANCE
EUROSYSTÈME

1. Rappel des textes de référence

2. Rôles de la Banque de France et des centres d'évaluation

3. Les objectifs de sécurité

DÉCRET N°2018-1228 DU 24 DÉCEMBRE 2018

- Art. D.133-10 […]

« *Les prestataires de services de paiement gestionnaires de comptes qui souhaitent bénéficier de l'exemption*

adressent à l'Autorité de contrôle prudentiel et de résolution une demande comportant : […]

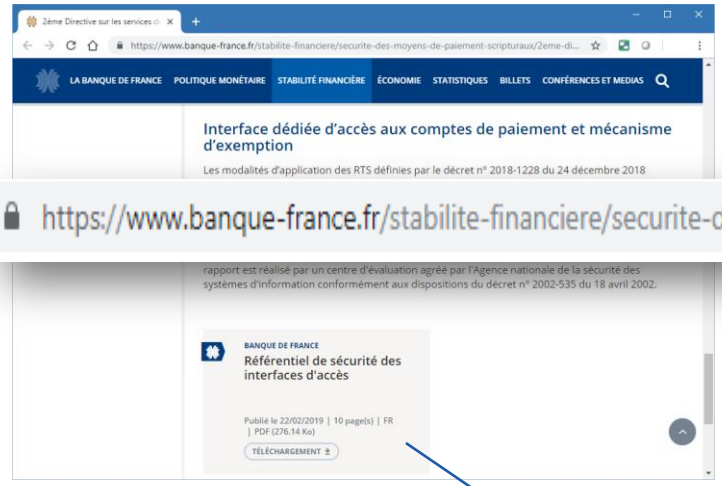
« *5° Un rapport attestant de la conformité de l'interface dédiée aux dispositions sur la sécurité prévues par ce même règlement délégué et détaillées par un référentiel sur la sécurité établi par la Banque de France en application de l'article L. 521-8 du présent code.*

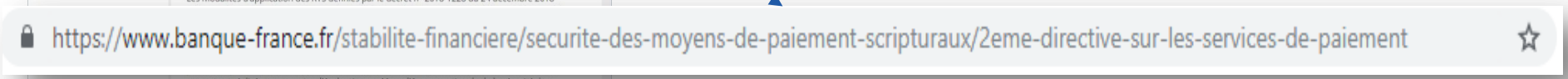
DÉCRET N°2018-1228 DU 24 DÉCEMBRE 2018

- Le rapport de conformité est réalisé par un **centre d'évaluation** agréé par l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** conformément aux dispositions du décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

- <u>Ce qu'il faut retenir</u>
  - Les centres d'évaluation peuvent utiliser la méthodologie de leur choix pour réaliser l'audit
  - La structure du rapport de conformité doit suivre au plus près celle du référentiel de sécurité, ou qu'une correspondance claire et linéaire soit présente au sein du rapport (à minima, en annexe)
  - Après analyse, ce rapport servira à la Banque de France pour émettre son avis à l'ACPR

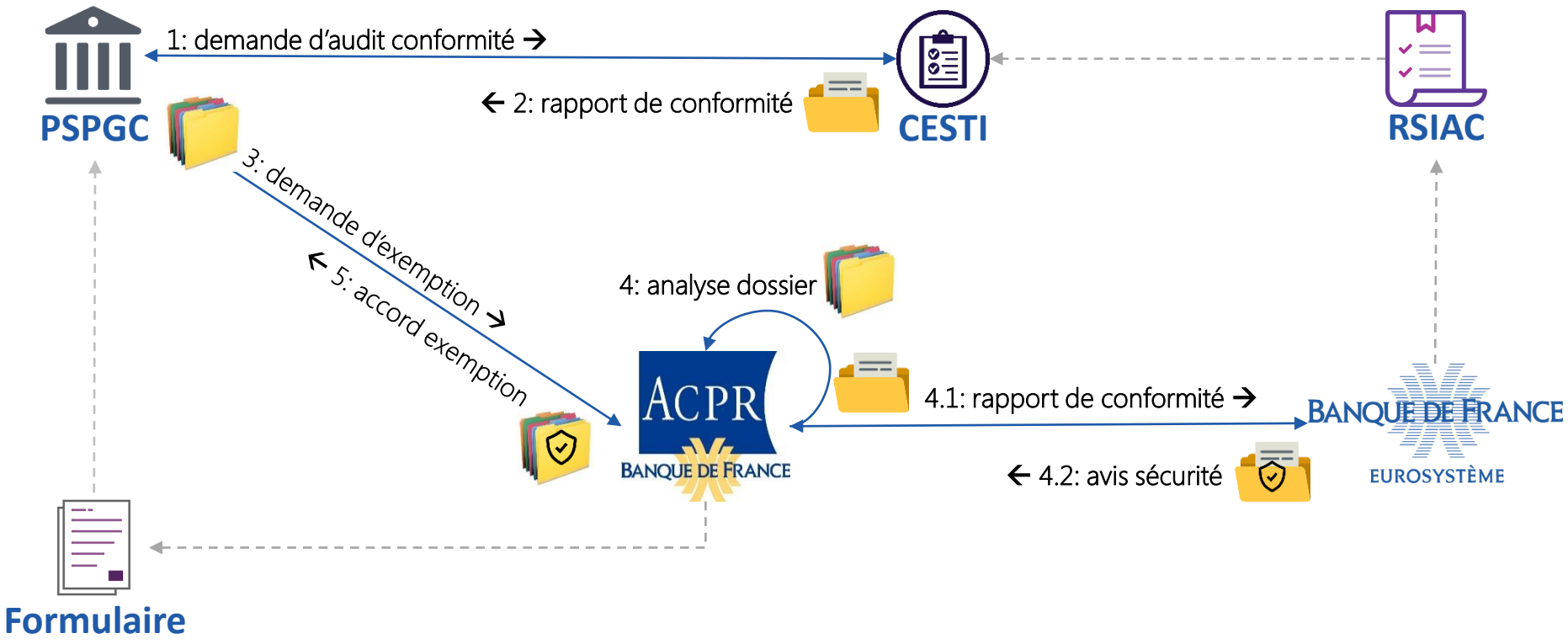
RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES (RSIAC)





BANQUE DE FRANCE
EUROSYSTÈME

RÔLES DES ACTEURS IMPLIQUÉS



**PSPGC: Prestataire de services de paiement gestionnaire de compte*

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- **Objectifs de sécurité**

1. Gouvernance et organisation
2. Évaluation des risques
3. Contrôle et encadrement des risques
4. Identification
5. Sécurité des flux et des sessions de communication
6. Traçabilité
7. Interopérabilité

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- **Objectifs de sécurité**

1. Gouvernance et organisation
2. Évaluation des risques
3. Contrôle et encadrement des risques

- *[EXG 1.1] La politique de gouvernance des interfaces d'accès […] est formalisée par les prestataires de services gestionnaires de comptes et régulièrement actualisée. Elle définit le cycle de vie ainsi que la politique de sécurité globale de ces API.*
- *[EXG 3.1] Les prestataires de services de paiement gestionnaires de comptes s'assurent de la mise en œuvre de mesures de sécurité adaptées à la nature et l'importance des risques identifiés […]*

- Ce qu'il faut retenir
  - Gestion du cycle de vie des API
  - Gestion et maîtrise des risques sécurité

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- Objectif de sécurité 4 : Identification
- *[EXG 4.2] Les prestataires de services de paiement gestionnaires de comptes s'assurent que les prestataires de services de paiement tiers utilisent un certificat qualifié d'authentification de site internet pour sécuriser la couche de transport et un certificat qualifié de cachet électronique pour signer électroniquement le contenu des messages échangés.*

- Ce qu'il faut retenir
  - Utilisation de certificats qualifiés QWAC et/ou QSealC
  - Être en capacité de contrôler la validité en cours des certificats et des agréments

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- Objectif de sécurité 5 : Sécurité des flux et des sessions de communication
- *[EXG 5.7] Les prestataires de service de paiement gestionnaires de comptes garantissent l'intégrité et la confidentialité des données de sécurité personnalisées et des codes d'authentification qui transitent par les flux de communication ou qui sont stockés dans l'infrastructure technique de leurs systèmes d'information.*
- *[EXG 5.8] Les sessions de communication entre le prestataire de services de paiement gestionnaire du compte, le prestataire de services d'information sur les comptes, le prestataire de services d'initiation de paiement et tout utilisateur de services de paiement concerné sont établies et maintenues tout au long de l'authentification.*

- Ce qu'il faut retenir
  - Les flux sont sécurisés au niveau des couches transport et application
  - Les flux sont supervisés
  - Les flux et les données sont chiffrés

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- Objectif de sécurité 6 : Traçabilité
- *[EXG 6.1] […] b. des mécanismes de sécurité pour l'enregistrement détaillé de l'opération, y compris le numéro de l'opération, les horodatages et toutes les données pertinentes de l'opération; […]*
- *[EXG 6.3] En cas d'erreur ou d'événement imprévu […], le prestataire de services de paiement gestionnaire du compte envoie un message de notification au prestataire de services (tiers) […] en indiquant les raisons de l'erreur ou de l'événement imprévu.*

- Ce qu'il faut retenir
  - Piste d'audit
  - Messages d'erreur détaillés

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES

- Objectif de sécurité 7 : Interopérabilité
- *[EXG 7.1] Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leurs interfaces d'accès suivent des normes de communication publiées par des organisations européennes ou internationales de normalisation.*
- *[EXG 7.2] Les prestataires de services de paiement gestionnaires de comptes veillent à ce que les spécifications techniques des interfaces d'accès fassent l'objet d'une documentation […] pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes des prestataires de services de paiement gestionnaires de comptes.*

- Ce qu'il faut retenir
  - Documentation des API
  - Application des normes