Projet test24/06/199801/06/199801/01/1998



GUICHET ONEGATE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notice descriptive des étapes de votre accréditation à ONEGATE-OSCAMPS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

COLLECTES OSCAMPS

VERSION 2 -12/12/2014



DGO-DSPM-SEMOP

**SUIVI DES VERSIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Commentaire | Rédacteur |
| **1.0** | 10/06/2014 | Livraison du document | **Équipe projet OSCAMPS** |
| **2.0** | 12/12/2014 | Refonte du document | **Équipe projet OSCAMPS** |

**TABLE DES MATIERES**

[1 Préambule 4](#_Toc406158688)

[2 Terminologie 4](#_Toc406158689)

[3 Cinématique de votre accréditation à ONEGATE-OSCAMPS 5](#_Toc406158690)

[3.1 Étape 1 : Demander votre certificat d’authentification 5](#_Toc406158691)

[3.2 Étape 2 : Installer votre certificat issu de la Banque de France 6](#_Toc406158692)

[3.3 Étape 3 : Vous accréditer à ONEGATE-OSCAMPS 6](#_Toc406158693)

[4 SUPPORT assuré par la Banque de France 6](#_Toc406158694)

# Préambule

**L’accès à ONEGATE-OSCAMPS nécessite l’installation sur votre poste de travail d’un certificat d’authentification personnelle simple. Ce certificat d’authentification personnel doit ensuite être déclaré au support ONEGATE pour que vous puissiez accéder à l’application ONEGATE-OSCAMPS.**

**Le présent document s’adresse à des utilisateurs standards. Il présente les différentes étapes de votre accréditation.**

# Terminologie

**Certificat**: un certificat est une carte d'identité numérique personnelle principalement utilisée pour identifier et authentifier une personne physique ou morale, mais aussi pour [chiffrer](http://fr.wikipedia.org/wiki/Chiffrer) des échanges. Il est [signé](http://fr.wikipedia.org/wiki/Signature_num%C3%A9rique) par un [tiers de confiance](http://fr.wikipedia.org/wiki/Tiers_de_confiance) qui atteste du lien entre l'identité physique et l'entité numérique ([Virtuel](http://fr.wikipedia.org/wiki/Virtuel)). Lorsqu'un diffuseur d'informations (vous) veut diffuser une clé publique pour être authentifié par une application, il contacte une autorité de certification (AC) qui va recevoir la clé publique et l'identité du diffuseur. Après avoir vérifié l'identité du demandeur par des moyens conventionnels, l'AC place l'identité et la clé publique fournie dans un conteneur qu'elle signe en utilisant sa clé privée. Le fichier résultant est le certificat qui est rendu au diffuseur.

**Code de révocation :** le code de révocation constitue un mot de passe défini lors de la demande de certificat auprès de l’AC. Ce code sera demandé lors du retrait du certificat.

**AC** : l’Autorité de certification a pour mission, après vérification de l'identité du demandeur du certificat par une autorité d'enregistrement (AE), de signer, émettre et maintenir :

* les certificats (CSR : *Certificate Signing Request*) ;
* les listes de révocation (CRL : [*Certificate Revocation List*](http://fr.wikipedia.org/wiki/Liste_de_r%C3%A9vocation_de_certificats)).

**AE**: l’Autorité d’enregistrement vérifie, conformément à la politique de certification, que :

* les demandeurs ou les porteurs de certificat sont identifiés ;
* l’identité des demandeurs est authentique ;
* les contraintes liées à l’usage d’un certificat sont remplies.

**Mandataires de Certification :** Les mandataires de certification sont les personnes habilitées à demander des certificats. Ils s’engagent à effectuer correctement et de manière approfondie les contrôles d’identité des futurs porteurs sous leur responsabilité et à respecter les parties de la [Politique de Certification](http://ae.certificats.banque-france.org/igc-bdf-v2/pc/feuille/sig-pers-1-1.2.250.1.115.200.2.1.2.4.1.1.1) qui leur incombent.

Bien qu’ils jouent le rôle particulier d’Autorité d’Enregistrement déléguée, les Mandataires de Certification n’ont pas accès aux données d’activation des porteurs. Ainsi, ils ne sont pas en mesure d’utiliser les clés privées des porteurs.

**Chaine de confiance** : En pratique, la certification peut s'effectuer en cascade : un certificat peut permettre d'authentifier d'autres certificats jusqu'au certificat qui sera utilisé pour la communication. La Banque de France est constituée d’une chaine de confiance d’AC.

**Liste de révocation de certificats :** (CRL, *certificate revocation list*) est la liste des identifiants des certificats qui ne sont plus dignes de confiance (certificats révoqués ou qui ne sont plus valables). Un certificat peut devenir invalide pour de nombreuses raisons autres que l'expiration naturelle, telle que la perte ou la compromission de la clé privée associée au certificat ou le changement d'au moins un champ inclus dans le nom du titulaire/ détenteur du certificat.

# Cinématique de votre accréditation à ONEGATE-OSCAMPS

## Étape 1 : Demander votre certificat d’authentification

ONEGATE a mis en place une politique de multi-acceptation qui permet de se connecter au portail avec des certificats reconnus par des autorités référencées :

* PAC (Politique d’Acceptation Commune) : Politique définie par le secteur bancaire pour le secteur bancaire, afin de répondre aux besoins des promoteurs d’applications du secteur bancaire. La liste des autorités référencées peut être trouvée à l’adresse suivante : <http://www.cfonb.org/Default.aspx?lid=1&rid=122&rvid=148>
	+ RGS (Référentiel Général de Sécurité) : Référentiel étatique qui décrit les exigences de sécurité sur les certificats pour les échanges entre administration et citoyens. La liste des autorités référencées peut être trouvée à l’adresse suivante : <http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe>
	+ Banque de France : En sa qualité d'Autorité de Certification, la Banque de France délivre des certificats numériques afin de sécuriser les échanges avec ses propres partenaires. Des informations complémentaires peuvent être obtenues à l’adresse suivante : <http://www.banque-france.fr/igcbdf>.
	**IMPORTANT : Les certificats permettant de se connecter au portail POBI de la Banque de France ne permettent pas de se connecter à ONEGATE-OSCAMPS.**

Si vous ne disposez pas déjà d’un certificat d’authentification provenant des autorités de certification ci-dessus, votre mandataire de certification devra déposer une demande de certificat (**un certificat et un seul par remettant à accréditer**) auprès de l’autorité de son choix décrite dans l’énumération ci-dessus.

Les demandes auprès de la Banque de France doivent être retournées par mail au support ONEGATE: onegate-support@banque-france.fr. Le document **Accréditations- 20\_Formulaire Demande Certificat BDF.docx** est disponible sur le site e-Oscamps (<https://oscamps.banque-france.fr/accueil/documentation-collectes/documents-techniques.html>).

**NOTA : L’utilisation d’un certificat existant (autre qu’un certificat POBI) vous permet d’éviter cette étape et de passer directement à l’étape d’accréditation à ONEGATE-OSCAMPS.**

## Étape 2 : Installer votre certificat issu de la Banque de France

Si vous choisissez de ne pas demander votre certificat à votre autorité de certification mais à la Banque de France, vous trouverez une aide à l’installation du certificat Banque de France dans la notice d’installation (**Accréditations - 10\_Notice Installation Certificat BdF.docx**) disponible sur le site e-Oscamps (<https://oscamps.banque-france.fr/accueil/documentation-collectes/documents-techniques.html>).

## Étape 3 : Vous accréditer à ONEGATE-OSCAMPS

**Une fois votre certificat retiré et installé**, celui-ci doit être déclaré à ONEGATE par le biais de l’accréditation à ONEGATE-OSCAMPS pour que vous puissiez accéder à l’application. Vous trouverez la notice d’accréditation (**Accréditations - 30\_Notice Accréditation.docx**) disponible sur le site e-Oscamps (<https://oscamps.banque-france.fr/accueil/documentation-collectes/documents-techniques.html>).

# SUPPORT assuré par la Banque de France

Au-delà des renseignements techniques que vous pouvez requérir en interne, les renseignements sur cette procédure peuvent être obtenus par sollicitation du support ONEGATE : onegate-support@banque-france.fr.

**[FIN DU DOCUMENT]**