MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

Service d'émission de certificats de personnes qualifié des ministères économiques et financiers

AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE
(OID 1.2.250.1.131.1.11.6.3.1.1)

Conditions Générales d'Utilisation (PKI Disclosure Statement)

V1.4- Diffusion : publique

TABLE DES MATIERES

1 OBJET DU DOCUMENT

Le présent document constitue les conditions générales d'utilisation des certificats délivrés par l'Autorité de Certification « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » des ministères économiques et financiers (MEF).

Ce document présente, en synthèse, les dispositions de la Politique de Certification de l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » des MEF, identifiée par l'OID 1.2.250.1.131.1.11.6.3.1.1, en particulier les modalités d'utilisation des certificats ainsi que les engagements et responsabilités respectives des différents acteurs concernés.

2 DEFINITIONS ET ACRONYMES

Autorité de certification (AC)	Une Autorité de Certification a en charge l'application d'au moins une politique de certification (PC) et est identifiée comme telle, en tant qu'émetteur (*champ "issuer" du certificat*), dans les certificats émis au titre de la politique de certification.
Autorité d'enregistrement (AE)	L'AE applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans le certificat.
Liste des certificats révoqués (LCR) ou Certificate Revocation List (CRL).	Liste des numéros de certificats ayant fait l'objet d'une révocation. La LCR est signée par l'autorité de certification pour assurer son intégrité et son authenticité.
Déclaration des pratiques de certification (DPC)	Ensemble des pratiques à mettre en œuvre pour satisfaire aux exigences de la PC.
Politique de certification (PC)	Ensemble de règles qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs.
Porteur	Un porteur de certificats ne peut être qu'une personne physique. Le porteur est un agent des MEF ou une personne externe liée contractuellement aux MEF qui utilise sa clé privée et le certificat électronique associé pour ses activités en lien avec l'entité, identifiée dans le certificat électronique, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire.
Mandataire de Certification (MC)	Le MC est une personne ayant, directement par la loi ou par délégation, le pouvoir d'autoriser une demande de certificat portant le nom de l'organisation. Il peut aussi avoir d'autres pouvoirs au nom de l'organisation, comme celui de révocation.

AC	Autorité de certification
AE	Autorité d'enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CS	Comité de Surveillance
CN	Common Name
CRL	Certificate Revocation List, ou LCR
DPC	Déclaration des Pratiques de Certification
eIDAS	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
LAR	Liste des certificats d'AC révoqués, ou ARL
LCR	Liste des Certificats Révoqués
MC	Mandataire de certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de certification
PDS	PKI Disclosure Statement (*Déclaration des informations du service d'émission de certificats*)
PSCE	Prestataire de services de certification électronique
QSCD	Qualified Signature Creation Device (Dispositif de création de signature qualifié)
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
SSI	Sécurité des systèmes d'information
URL	Uniform Resource Locator

3 CONDITIONS GENERALES D'UTILISATION

Contact de l'Autorité de Certification	Ministères économiques et financiers Secrétariat général 139, rue de Bercy 75572 Paris Cedex 12 Contact-igc-mef@finances.gouv.fr
Type de certificats émis	L'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » délivre des certificats double usage authentification et signature qualifiés au sens du RGS pour le niveau de sécurité 2 étoiles (**) et qualifiés au sens du règlement eIDAS. Le certificat double usage authentification et signature est référencé sous l'OID de la PC : 1.2.250.1.131.1.11.6.3.1.1. Les certificats sont émis conformément à la politique de certification publiée aux adresses suivantes : • https://igc.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf • https://igc1.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf • https://igc2.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf Les certificats sont émis à travers la chaîne de certification suivante : **AC RACINE MEF QUALIFIEE** **|** **AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE**
Objet des certificats	Les certificats double usage authentification et signature émis par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » sont des certificats stockés dans un dispositif matériel de type QSCD à destination de personnes physiques : • Agents des MEF, • Prestataires externes intervenant au sein des MEF.
Durée / entrée en vigueur	Les présentes CGU sont opposables au porteur dès leur acceptation et, à défaut dès la première utilisation du certificat. Les CGU sont opposables pendant toute la durée de vie du certificat d'une période de trois ans pour les certificats double usage authentification et signature sans préjudice de leurs éventuelles mises à jour. L'AC s'engage à communiquer par tous moyens à sa disposition (*courrier électronique, information en ligne, etc.*) toute nouvelle version des CGU.

	Toute utilisation du certificat après les modifications ou la mise à jour des CGU vaut acceptation des nouvelles CGU par le porteur.
Modalités d'obtention	**Validation initiale de l'identité** Une demande de certificat ne peut être effectuée que par un des acteurs ci-dessous : • Le futur porteur, • Un MC, • L'AE, L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un Mandataire de Certification (MC). Dans ce dernier cas, le MC est préalablement enregistré par l'AE. La vérification et la validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants : • Enregistrement d'un porteur sans MC : validation par l'AE de l'identité « personne morale » de l'entité de rattachement du porteur et de l'identité « personne physique » du futur porteur. • Enregistrement d'un MC : validation de l'identité « personne morale » de l'entité pour lequel le MC interviendra et de l'identité « personne physique » du futur MC. • Enregistrement d'un porteur via un MC : validation par le MC de l'identité « personne physique » du futur porteur. L'AC prévoit de délivrer : • Des certificats sur une carte « *agent* » pour les agents présents sur le référentiel des agents des MEF et ne nécessitant pas l'intervention d'un MC, • Des certificats sur une carte « *temporaire* » pour : o Les agents présents sur le référentiel des agents des MEF qui ne nécessitent pas l'intervention d'un MC, o Les agents inconnus dans le référentiel des agents des MEF (ex : nouveaux arrivants) et nécessitant donc l'intervention d'un MC et la constitution d'un dossier de demande de certificat, o Les prestataires externes, par définition inconnus dans le référentiel des agents des MEF (*même s'ils peuvent apparaître dans l'annuaire de référence de l'AE*), et nécessitant l'intervention d'un MC et la constitution d'un dossier de demande de certificat. **Demande de certificat** La demande de certificat contient *à minima* les informations suivantes : • Le nom du porteur à utiliser dans le certificat, • Les données personnelles d'identification du porteur, • Les données de l'entité du porteur. **Délivrance du certificat** La personnalisation du dispositif matériel de type QSCD du porteur et la délivrance du certificat sont réalisées par l'AE en présence du porteur qui récupère à l'issue de cette séance son dispositif matériel personnalisé (sa carte) contenant ses certificats.

	Acceptation du certificat Le certificat généré à l'issue de la personnalisation du dispositif matériel est présenté au porteur pour validation de son contenu. L'acceptation du certificat par le porteur est recueillie par un bouton « Valider ».
Modalités d'activation/de déblocage de la carte	**Activation de la carte** L'activation de la clé privée du porteur contenue dans la carte nécessite la saisie du code PIN de la carte, défini par le porteur lors de l'obtention du certificat et qui est sous son contrôle exclusif. **Déblocage de la carte** En cas de blocage de la carte faisant suite à plusieurs tentatives successives erronées de saisie du code PIN, l'AC met à disposition du porteur exclusivement un service de déblocage de carte. Pour toute demande de déblocage de carte, le porteur doit se rapprocher d'un opérateur de déblocage habilité.
Modalités de renouvellement	Une notification est envoyée au porteur à l'approche de la date d'expiration du certificat de façon à préparer la délivrance d'un nouveau certificat. Le déclenchement de la fourniture d'un nouveau certificat au porteur se fait à l'initiative du porteur. Le processus de renouvellement ne concerne que la carte « *agent* » et non la carte « *temporaire* » qui doit suivre le même processus qu'une demande initiale. Lors du premier renouvellement, la vérification de l'identité du sujet est optionnelle. S'il n'y a aucune modification portant sur les identités identifiées, la liste des documents à fournir est allégée. Dans ce cadre, le porteur peut réaliser l'opération seul en s'authentifiant avec l'ancien certificat toujours en cours de validité. Lors du renouvellement suivant, l'AE, saisie de la demande, identifie le sujet selon la même procédure que pour l'enregistrement initial. Note : La génération d'une nouvelle bi-clé est systématique pour toute délivrance d'un certificat.
Modalités de révocation	**Identification et validation d'une demande de révocation** Une demande de révocation d'un certificat émis par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » peut être faite par : • Le porteur lui-même, • Un MC ou un représentant légal de l'entité du porteur ou une personne autorisée, • L'AE, • L'AC. La demande de révocation peut être effectuée : • Sur Internet si le porteur dispose d'un moyen d'authentification au portail Self-service,

- En face-à-face entre le porteur et l'AE au cours duquel le porteur présente un document officiel d'identité,
- Via un centre d'appel en fonction de l'AE,
- Par courriel ou par courrier (*en fonction de l'AE*), la demande doit être signée par le demandeur.
  Le formulaire de révocation est disponible sur les sites de publication igc.finances.gouv.fr, igc1.finances.gouv.fr, igc2.finances.gouv.fr.
  Ci-dessous les adresses de chaque direction endossant le rôle d'AE dans le cadre de la PC associée aux présentes CGU :

Direction des MEF	Contacts
DGDDI	**Par courriel :** *revocation-dgddi.ac-mef@douane.finances.gouv.fr* **Par courrier :** *Direction générale des douanes et droits indirects* *SDSI / Bureau SI2* *11 RUE DES DEUX COMMUNES* *93558 MONTREUIL*
Administration Centrale	**Centre de service** *88000.finances.gouv.fr* *MEFSIN* *Service du numérique* *MCTI* *139 rue de Bercy* *75012 PARIS CEDEX 12*

Demande de révocation

La demande de révocation comporte au moins les informations suivantes :

- L'identité du porteur figurant dans le certificat (*nom et prénom*),
- Le nom du demandeur de la révocation,
- Une information permettant de retrouver rapidement et sans erreur le certificat à révoquer (*par défaut le n° de série*),
- Eventuellement, la cause de révocation.

Traitement d'une demande de révocation

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

Notification de la révocation

	Quelle que soit la cause ayant entraîné la révocation d'un certificat, le porteur est informé par une notification de la révocation de son certificat. Le MC peut également être notifié. Cette notification prend la forme d'un courrier électronique et indique la date à laquelle la révocation du certificat a pris effet.
Fin de vie de l'AC	Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC. Les dispositions prises par l'AC en cas de cessation de service comprennent : • La notification des entités affectées, • Le transfert de ses obligations à d'autres parties, • La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés. Lors de l'arrêt du service, l'AC : • Informe tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant. • Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité, • Génère une dernière LCR couvrant la révocation des certificats cités plus-haut et signée par la clé privée de l'AC. La valeur de l'extension nextUpdate de la dernière LCR alors émise est alors « *99991231235959Z* », • Génère pour chaque certificat émis, une dernière réponse OCSP dont la fin de validité est positionnée au 31 décembre 9999, 23h59m59s (*« 99991231235959Z »*), • S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats, • Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante, • Révoque son certificat,
Obligations du porteur	Le porteur a l'obligation de : • Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat, • Protéger sa clé privée par des moyens appropriés à son environnement, • Protéger ses données d'activation et, le cas échéant, les mettre en œuvre, • Protéger l'accès à sa base de certificats, • Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant, • Informer l'AC de toute modification concernant les informations contenues dans son certificat, • Faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entité le cas échéant ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (*ou de ses données d'activation*). • En cas de dysfonctionnement de la carte portant la clé privée, que ce dysfonctionnement soit lié à l'utilisation de la clé privée ou à une fonctionnalité

	annexe de la carte, de se rapprocher de l'AE pour que l'AE mette au rebut de la carte et révoque le certificat correspondant.
Obligations de vérification des certificats par les utilisateurs	Les utilisateurs de certificats ont l'obligation de : • Vérifier et respecter l'usage pour lequel un certificat a été émis, • Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (*dates de validité, statut de révocation*), • Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans les présentes Conditions Générales d'Utilisation, Les certificats de la chaîne de certification sont disponibles auxadresses suivantes : Pour l'AC « *AC RACINE MEF QUALIFIEE* » : • https://igc.finances.gouv.fr/ac-racine-mef-qualifiee.cer • https://igc1.finances.gouv.fr/ac-racine-mef-qualifiee.cer • https://igc2.finances.gouv.fr/ac-racine-mef-qualifiee.cer Pour l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIE* » : • https://igc.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer • https://igc1.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer • https://igc2.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer La liste de révocation des certificats émise par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » est disponible auxadresses suivantes : • http://crl.igc.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl • http://crl.igc1.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl • http://crl.igc2.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl En complément, un service de vérification en ligne du statut des certificats (OCSP) est mis à disposition des utilisateurs. Le répondeur OCSP est accessible à l'adresse suivante : • http://ocsp-ac-mef.finances.gouv.fr/ac-online-mef-qualifiees/ http://ocsp-ac-mef.finances.rie.gouv.fr/ac-online-mef-qualifiees/
Limites de responsabilité	Les porteurs doivent respecter les conditions d'utilisation de leur clé privée et du certificat correspondant.

	Les utilisateurs de certificat doivent vérifier et respecter l'usage pour lequel un certificat a été émis. Le MEFR décline toute responsabilité dans l'usage fait d'un certificat dans un cadre autre que les usages prévus ci-dessous : • Les certificats émis par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » pour des personnes physiques ne sont utilisables qu'à des fins d'authentification et de signature électronique. Les certificats émis par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » sont délivrés pour une durée de 3 ans.
Limite de garantie	Sous réserve des dispositions d'ordre public applicables, les ministères économiques et financiers ne pourront pas être tenus responsables d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR et des LCR ainsi que de tout autre équipement ou logiciel mis à disposition. Les ministères économiques et financiers déclinent en particulier leur responsabilité pour tout dommage résultant : • D'un emploi des bi-clés pour un usage autre que ceux prévus, • De l'usage de certificats révoqués ou expirés, • De l'absence de demande de révocation d'un certificat entraînant l'utilisation du certificat et de la bi-clé par un tiers non autorisé, • D'un cas de force majeure tel que défini par les tribunaux français. Les ministères économiques et financiers déclinent également leur responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.
Références documentaires	La Politique de Certification de l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » est accessible aux adresses suivantes : • https://igc.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf • https://igc1.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf • https://igc2.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf
Politique de confidentialité	La collecte et l'usage de données personnelles par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (règlement général sur la protection des données – RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. Les dossiers d'enregistrement sont conservés 7 ans pour des besoins de fourniture de preuves.

	De même les journaux d'évènements du CMS ROSSIGNOL sont conservés 7 ans après leur génération. A l'issue de la durée de l'archivage, les données font l'objet d'une destruction.
Conditions d'indemnisation	Sans objet
Loi applicable / résolution de conflits	Les présentes CGU et la Politique de Certification de l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » sont soumises au droit français. En cas de litige le porteur prend attache avec le service d'assistance aux utilisateurs de son entité (via un appel téléphonique ou via une interface web dédiée). Cette action est tracée dans un outil permettant de suivre le traitement.
Audits et références applicables	Les certificats émis par l'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » bénéficient d'une qualification au sens du RGS et d'une qualification au sens du Règlement eIDAS. Ces offres de certificats et la politique de certification associée sont conformes : • Aux exigences du RGS pour le niveau 2 étoiles, • Et au document ETSI EN 319 411-2, portant les exigences incombant aux autorités de certification délivrant des certificats qualifiés au sens du Règlement eIDAS, pour le profil QCP-N-QSCD. Un contrôle de conformité de la PC pourra être effectué, sur demande du Comité de Surveillance. L'AC s'engage à effectuer ce contrôle au minimum une fois tous les deux ans. Par ailleurs, avant la première mise en service d'une composante du service d'émission de certificats ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante.