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

General Administration

Qualified certificate issuance service of the economic and financial ministries

MEF QUALIFIED AUTHENTICATION AND SIGNATURE CA (*OID* 1.2.250.1.131.1.11.6.3.1.1)

Terms and Conditions (PKI Disclosure Statement)

V1.4 - Distribution: public

TABLE OF CONTENTS

1 PURPOSE OF THE DOCUMENT

This document constitutes the general terms and conditions for the use of certificates issued by the "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" Certification Authority of the ministries for the economy and finance (MEF).

This document contains a summary of the provisions of the Certification Policy of the "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" CA of the MEF, identified by OID 1.2.250.1.131.1.11.6.3.1.1, including the terms of using certificates as well as the respective commitments and responsibilities of the various stakeholders in question.

2 DEFINITIONS AND ACRONYMS

Certification Authority (CA)	A Certification Authority is in charge of at least one certification policy (CP) and is identified as such, as an issuer (in the "issuer" field of the certificate) in certificates issued under the certification policy.
Registration Authority (RA)	The RA applies procedures to identify natural persons or legal entities, in accordance with the rules imposed by the Certification Authority. Its purpose is to establish that the applicant has the identity and capacity stated in the certificate.
Certificate Revocation List (CRL)	List of certificate numbers that have been revoked. The CRL is signed by the certification authority to ensure its integrity and authenticity.
Certification Practice Statement (CPS)	All practices to be carried out in order to meet the requirements of the CP.
Certification Policy (CP)	Set of rules that sets out the conditions governing the applicability of a certificate for a given community or for applications with common security requirements.
Holder	A certificate holder must be an individual. The holder is an agent of the MEF or an external person contractually bound to the MEF who uses their private key and the associated electronic certificate for their activities relating to the entity identified on the electronic certificate, with which they have a contractual, hierarchical or regulatory relationship.
Certification Agent (CAg)	The CAg is a person who, by law or by delegation, has the authority to authorise applications for certificates bearing the name of the organisation. They may also have other powers to act on behalf of the organisation, such as the revocation of certificates.

CA	Certification Authority
RA	Registration Authority
ANSSI	Agence nationale de la sécurité des systèmes d'information (French National Information Systems Security Agency)
SC	Supervisory Committee
CN	Common Name
CRL	Certificate Revocation List
CPS	Certification Practice Statement
eIDAS	Regulation No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
ARL	Authority Revocation List
CRL	Certificate Revocation List
CAg	Certification Agent
OCSP	Online Certificate Status Protocol
OID	Object Identifier
CP	Certification Policy
PDS	PKI Disclosure Statement
ECSP	Electronic Certification Service Provider
QSCD	Qualified Signature Creation Device
GDPR	General Data Protection Regulation
RGS	Référentiel Général de Sécurité (French General Security Guidelines)
ISS	Information System Security
URL	Uniform Resource Locator

3 GENERAL TERMS AND CONDITIONS OF USE

Contact details of the Certification Authority	Ministère de l'Economie, des Finances et de la Relance Secrétariat général [General Administration] 139, rue de Bercy 75572 Paris Cedex 12 Contact-igc-mef@finances.gouv.fr
Type of certificates issued	The "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" CA issues dual use qualified authentication and signature certificates within the meaning of the RGS for the 2-star (**) security level and qualified within the meaning of the eIDAS regulation. The dual use authentication and signature certificate has the following OID reference under the CP: 1.2.250.1.131.1.11.6.3.1.1. Certificates are issued in accordance with the certification policy published at the following address: • 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 Certificates are issued through the following certificate chain: **AC RACINE MEF QUALIFIEE** | **AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE**
Purpose of the certificates	The dual use authentication and signature certificates issued by the "*MEF QUALIFIED AUTHENTICATION AND SIGNATURE CA*" CA are certificates stored in hardware such as a QSCD intended for natural persons who are: • MEF Agents, • External service providers working at the MEFs.
Term/Effective Date	These General Terms and Conditions of Use shall be binding on the holder following acceptance and, failing this, when the certificate is first used. The General Terms and Conditions of Use are enforceable throughout the certificate's three-year term for dual use authentication and signature certificates, without prejudice to any updates thereto. The CA undertakes to communicate using any means available to it (*email, online notification, etc.*) any new version of the General Terms and Conditions of Use.

By using the certificate after amendments or updates are made to the General Terms and Conditions of Use, the holder is deemed to have accepted the new General Terms and Conditions of Use.

Procedures for obtaining certificates

Initial validation of identity

An application for a certificate may only be made by one of the following persons:

- The future holder,
- A CAg,
- The RA,

A holder may register directly with the RA or via a Certification Agent. In the latter case, the CAg must first be registered with the RA.

The verification and initial validation of the identity of an entity or individual is carried out in the following cases:

- Registration of a holder without a CAg: validation by the RA of the “legal entity” identity of the holder’s connected entity and the “individual” identity of the future holder.
- Registration of a CAg: validation of the “legal entity” identity of the entity for which the CAg will operate and the “individual” identity of the future CAg.
- Registration of a holder via a CAg: validation by the CAg of the “individual” identity of the future holder.

The CA proposes to issue:

- Certificates on an “*agent*” card for agents included on the MEFR’s list of agents who do not require the intervention of a CAg,
- Certificates on a “*temporary*” card for:
  - Agents included on the MEF’s list of agents who do not require the intervention of a CAg,
  - Agents who are not included on the MEF’s list of agents (for example, new joiners) who require the intervention of a CAg and need to apply for a certificate,
  - External service providers, who are by definition not included on the MEF’s list of agents *(even if they may be included in the RA’s reference directory*), who require the intervention of a CAg and need to apply for a certificate.

Application for a certificate

The application for a certificate must, at the very least, contain the following information:

- The name of the holder to be used in the certificate,
- The holder’s personal identification information,
- Information on the holder’s entity.

Issuance of the certificate

The customisation of the holder’s QSCD and the issuance of the certificate are carried out by the RA in the presence of the holder who, at the end of the meeting, receives his/her customised hardware device (card) containing his/her certificates.

	Acceptance of the certificate The certificate generated following customisation of the hardware device is presented to the holder for validation. The holder accepts the certificate by clicking on a “Validate” button.
How to activate and unlock the card	**Activating the card** The activation of the cardholder's private key contained in the card requires the entry of the PIN code of the card, defined by the cardholder when obtaining the certificate and which is under his exclusive control. **Unlocking the card** In the event of a card being blocked following several successive erroneous attempts to enter the PIN code, the AC shall make available to the cardholder exclusively a card unlocking service. For any request to unlock a card, the holder must contact an authorized unlocking operator.
Renewal procedures	A notification is sent to the holder close to the expiry date of the certificate so that a new certificate can be prepared for issue. The provision of a new certificate to the holder is triggered at the initiative of the holder. The renewal process covers only the “*agent*” card and not the “*temporary*” card, which must be applied for using the same process as for the initial application. When first renewed, the verification of the holder’s identity is optional. If there are no changes to the identified identities, the list of documents to be provided is reduced. Accordingly, the holder can simply carry out the operation themselves by authenticating their identity using the old certificate which remains valid. When next renewed, the RA, on receipt of the application, identifies the holder using the same procedure as for the initial registration. Note: A new key pair is systematically issued on the issue of a certificate.
Revocation procedures	**Identification and validation of a request for revocation** A request to revoke a certificate issued by the “*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*” CA may be made by: • The holder themselves, • A CA or legal representative of the holder’s entity or an authorised person, • The RA, • The CA. The request for revocation may be made: • On the Internet if the holder has a means of Self-service portal authentication • At a face-to-face meeting between the holder and the RA at which the holder presents an official identity document, • Via a call center depending on the RA, • By email or by post, the request must be signed by the applicant. The revocation form is available on the publication sites igc.finances.gouv.fr, igc1.finances.gouv.fr, igc2.finances.gouv.fr. Below are the addresses of each

department taking on the role of RA in the context of the associated Certificate Policy:

Department of the ministry	Contact
DGDDI	**By email :** *revocation-dgddi.ac-mef@douane.finances.gouv.fr* **By post :** *Direction générale des douanes et droits indirects* *SDSI / Bureau SI2* *11 RUE DES DEUX COMMUNES* *93558 MONTREUIL*
Administration Centrale	**Service center.** 88000@finances.gouv.fr*MEFSIN* *Service du numérique* *MCTI* *139 rue de Bercy* *75012 PARIS CEDEX 12*

Request for revocation
The request for revocation must, at the very least, contain the following information:

- The identity of the holder included on the certificate (*last name and first name*),
- The name of the person requesting the revocation,
- Information enabling the certificate that is to be revoked to be found quickly and accurately (*by default the serial number*),
- Possibly, the grounds for revocation.

Processing a revocation request
Once the application has been authenticated and checked, the revocation management function revokes the corresponding certificate by changing its status and then communicates this new status to the certificate status information function.

Notification of revocation
Regardless of the cause of a certificate being revoked, holders shall be notified of the revocation of their certificate. The CAg may also be notified. Such notification shall be sent by email and state the date on which the revocation of the certificate took effect.

Cessation of the CA's activities	In the event that it fully ceases its activities, the CA or, where that is impossible, any entity substitutes for it by law, a regulation, a court decision or an agreement previously entered into with that entity, shall revoke the certificates and the publication of the CRL in accordance with the commitments made in the CP.

	The actions to be taken by the CA in the event that it ceases providing its services include: • Notification of the affected entities, • The transfer of its obligations to other parties, • Managing the revocation status for non-expired certificates that have been issued. When the service is terminated, the CA shall: • Inform all CAgs and/or holders of certificates that have been revoked or are to be revoked, as well as any related entity. • Revoke all certificates it has signed where such certificates are still valid, • Generate a final CRL covering the revocation of the certificates referred to above signed by the CA's private key. The nextUpdate extension value of the last CRL issued is then "*99991231235959Z*", • Generate for each issued certificate a final OCSP response valid until 23:59:59 on 31 December 9999 ("*99991231235959Z*"), • Be prohibited from transmitting the private key that allowed it to issue certificates, • Take all necessary steps to destroy or render it ineffective, • Revoke its certificate,
Holders' Obligations	Holders are obliged to: • Provide accurate and up-to-date information when applying for or renewing the certificate, • Protect their private key using methods appropriate to their environment, • Protect their activation data and, where appropriate, use it, • Protect access to their certificate database, • Comply with the terms of use of their private key and the corresponding certificate, • Inform the CA of any change to the information included in their certificate, • Promptly ask the RA, the CAg for their entity, where applicable, or the CA to revoke their certificate, in the event that their private key (*or their activation data*) is compromised or they suspect that it has been compromised. • In case of malfunction of the card bearing the private key, whether this malfunction is related to the use of the private key or to an ancillary functionality of the card, to approach the AE so that the AE discards the card and revokes the corresponding certificate.
Obligations on users to verify certificates	Users of certificates are required to: • verify and comply with the use for which a certificate has been issued, • for each certification chain certificate, from the holder's certificate to the Root CA, verify the digital signature of the CA that has issued the certificate in question and check the validity of that certificate (*validity dates, revocation status*), • verify and comply with the obligations of users of certificates set out in these General Terms and Conditions of Use.

	Certification chain certificates are available at the following address: For the “*AC RACINE MEF QUALIFIEE*” CA: • 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 For the “*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIE*” CA: • 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 The certificate revocation list issued by the “*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIE*” CA is available at the following address: • 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 If access to the CRL is unavailable, an online certificate status protocol (OCSP) is available to users. The OCSP responder is available at the following address: • http://ocsp-ac-mef.finances.gouv.fr/ac-online-mef-qualifiees/
Limitation of liability	Holders must comply with the terms of use of their private key and the corresponding certificate. Users of certificates must verify and comply with the use for which a certificate has been issued. The MEFR shall not be held liable where a certificate is used for a purpose other than those set out below: • Certificates issued by the “*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*” CA for individuals can only be used for authentication and electronic signature purposes. Certificates issued by the “*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*” CA are issued for a period of 3 years.

Further limitations of liability	Subject to applicable public order provisions, the Ministry of the Economy, Finance and the Recovery may not be held liable for any unauthorised or non-compliant use of the certificates, the associated private keys and activation data, ARLs and CRLs as well as any other equipment or software made available. In particular, the Ministry of the Economy, Finance and the Recovery shall not be held liable for any losses resulting from: • the use of key pairs for any purpose other than those provided for, • the use of revoked or expired certificates, • the absence of a request for revocation of a certificate resulting in the use of the certificate and the key pair by an unauthorised third party, • an event of force majeure as defined by the French courts. The Ministry of the Economy, Finance and the Recovery shall also not accept any liability for any losses resulting from errors or inaccuracies in the information contained in the certificates, where such errors or inaccuracies are directly due to the information provided being incorrect.
Documentary references	The "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" CA's Certification Policy is available at the following address: • 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
Privacy policy	Personal data is collected and used by the CA and all its component parts in strict compliance with the laws and regulations in force in France, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable from 25 May 2018 (the General Data Protection Regulation - GDPR) and French data protection law no. 78-17 of 6 January 1978, as amended. Registration files are kept for 7 years to provide evidence. Similarly, CMS ROSSIGNOL event logs are kept for 7 years after their generation. At the end of the archiving period, the data is destroyed.
Conditions for paying compensation	N/A
Governing Law/Dispute Resolution	These General Terms and Conditions of Use and the "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" CA's Certification Policy shall be governed by French law.

	In the event of a dispute, the cardholder contacts his or her entity's user support service (by telephone or via a dedicated web interface). This action is traced in a tool enabling the processing to be tracked.
Audits and applicable references	The certificates issued by the "*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE*" CA are qualified within the meaning of the RGS and qualified within the meaning of the eIDAS Regulation. These offers of certificates and the associated certification policy meet: • the 2-star level requirements of the RGS, • and the ETSI EN 319 411-2 document on requirements for certification authorities that issue qualified certificates within the meaning of the eIDAS Regulation, for the QCP-N-QSCD profile. Compliance checks may be carried out on the CP at the request of the Supervisory Committee. The CA undertakes to perform such checks at least once every two years. In addition, before a component of the certificate issuing service is launched or following any significant change to a component, the CA will also carry out a compliance review on that component.