RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Extrait du
Bulletin Officiel des Finances Publiques-Impôts

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Identifiant juridique : BOI-TVA-DECLA-30-20-30-30-18/10/2013
Date de publication : 18/10/2013

TVA - Régimes d'imposition et obligations déclaratives et comptables - Règles relatives à l'établissement des factures - Factures électroniques - Factures transmises par voie électronique et sécurisées au moyen d'une signature électronique

Positionnement du document dans le plan :

Sommaire :

1

La signature électronique est un moyen de sécurisation des factures électroniques. Elle est susceptible de garantir l'authenticité de leur origine et l'intégrité de leur contenu.

Elle est une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données

électroniques et qui sert de méthode d'authentification du signataire et de l'origine des informations.

Elle a pour fonction d'identifier la personne qui l'appose et, le cas échéant, de manifester son accord. Elle permet, à l'aide d'un procédé cryptographique, de garantir l'identité du signataire. La signature électronique permet, en outre, de garantir l'intégrité de l'acte signé.

Un assujetti, qui signe électroniquement une facture électronique permet au destinataire de cette dernière d'en authentifier l'émetteur, d'y détecter une éventuelle atteinte à son intégrité (la facture a été modifiée) et, le cas échéant, d'attester la volonté de l'émetteur de donner son approbation aux dispositions contenues dans l'acte.

10

Différentes signatures électroniques existent et sont acceptées par l'administration fiscale aux fins de sécurisation des factures.

Parmi elles, seules la signature électronique avancée fondée par un certificat qualifié et créée par un dispositif sécurisé de création de signature et les signatures électroniques conformes au référentiel général de sécurité (RGS) de niveau 2 ou 3 étoiles garantissent de façon autonome l'authenticité de l'origine et l'intégrité du contenu des factures.

Les entreprises émettrices de factures assorties d'autres signatures électroniques (par exemple signature avancée au sens de l'article 2, point 2, de la directive 1999/93/CE du 13 décembre 1999 du Parlement européen, signature conforme au RGS une étoile...) doivent, aux fins de garantir l'authenticité de l'origine et l'intégrité du contenu des factures électroniques mettre également en place des contrôles établissant une piste d'audit fiable (BOI-TVA-DECLA-30-20-30-20).

I. Factures transmises par voie électronique et assorties d'une signature électronique « qualifiée »

20

On entend par signature électronique « qualifiée » une signature électronique avancée fondée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature électronique.

Conformément au 2° du VII de l'article 289 du code général des impôts (CGI), l'authenticité de l'origine, l'intégrité du contenu et la lisibilité d'une facture peuvent être assurées au moyen d'une telle signature sans aucune mesure complémentaire. Aucune piste d'audit fiable telle que définie au BOI-TVA-DECLA-30-20-30-20 n'est exigée.

A. Caractéristiques de la signature électronique « qualifiée »

30

La fiabilité d'une signature électronique est présumée jusqu'à preuve contraire lorsqu'elle est une signature électronique avancée, établie grâce à un dispositif sécurisé de création de signature et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Cette signature électronique dite « qualifiée » répond ainsi aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier.

Elle est recevable comme preuve en justice, au sens de l'article 1316-4 du code civil.

40

Les caractéristiques que doit présenter la signature électronique « qualifiée » sont définies à l'article 96 F de l'annexe III au CGI.

Aux termes du I de cet article, le signataire est une personne physique qui détient et met en œuvre le moyen de création de la signature électronique. Il agit pour son propre compte ou pour celui d'une personne physique ou morale qu'il représente.

50

Conformément à l'article 2, point 2, de la directive 1999/93/CE du 13 décembre 1999, la signature électronique avancée doit satisfaire aux exigences suivantes :

- être propre au signataire ;
- permettre d'identifier le signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir le lien avec les factures auxquelles elle s'attache, de telle sorte que toute modification ultérieure de ces factures soit détectable.

60

Elle peut être générée par des technologies de cryptographie asymétrique, c'est-à-dire des produits utilisant, en l'état de la technologie, deux clés distinctes (clé privée et clé publique) pour chiffrer puis déchiffrer un document.

70

En pratique, le signataire applique un algorithme d'empreinte du document d'origine, qui en constitue une version synthétique et unique. Le signataire utilise alors sa clé privée de signature (donnée de création de signature) pour chiffrer l'empreinte au moyen d'un algorithme cryptographique asymétrique et transmet le document d'origine et l'empreinte chiffrée au destinataire (la signature).

80

Le destinataire applique à son tour le même algorithme d'empreinte à partir du document d'origine et déchiffre l'empreinte chiffrée reçue avec l'algorithme cryptographique asymétrique au moyen de la clé publique (donnée de vérification de signature), associée de manière unique à la clé privée de signature et envoyée avec le message.

Le destinataire compare alors le résultat du déchiffrement avec l'empreinte qu'il a calculée : il s'agit de l'opération de vérification de la signature.

90

Enfin, pour être certain que la clé publique appartient bien à la personne ou à l'entreprise ayant signé le document, il est nécessaire d'avoir recours à un certificat électronique, document sous forme électronique signé par une tierce partie, encore appelée prestataire de service de certification, qui atteste de ce lien.

100

Dans l'hypothèse où plusieurs factures seraient transmises dans un même envoi, il est possible de signer l'ensemble des factures en cause et non chaque facture une à une dès lors qu'elles sont relatives à des opérations intervenues entre les mêmes assujettis.

B. Définition et caractéristiques du dispositif sécurisé de création de signature électronique

110

Le dispositif sécurisé de création de signature électronique doit garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

- ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
- ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification par les moyens techniques actuellement disponibles ;
- peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par d'autres personnes.

Il doit également n'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

120

Le dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au paragraphe précédent :

- dans les conditions prévues par le 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. La délivrance du certificat de conformité est rendue publique ;
- soit par un organisme désigné à cet effet par un État membre de l'Union européenne.

C. Définition et caractéristiques du certificat électronique qualifié

130

Un certificat électronique est une identité numérique. Il est nominatif, donc appartient personnellement à un membre d'une société. Le certificat électronique est constitué des deux éléments indissociables.

1. les informations indispensables

140

Les informations concernant l'identité du titulaire (nom, prénom, fonction, service, email…), son organisation (société, association…), la période de début et de fin de validité du certificat, l'identité de l'autorité de certification qui l'a généré, les fonctionnalités autorisées du certificat, l'adresse concernant l'accès à la politique de certification de l'autorité ainsi que l'adresse de la liste des certificats révoqués ;

2. la clé publique

150

Le certificat, nécessaire pour la réponse électronique, est constitué d'une clé publique. La clé privée associée à la clé publique doit rester secrète (on parle de cryptographie asymétrique) et être confinée dans un support matériel cryptographique : une clé USB cryptographique ou une carte à puce, par exemple.

L'autorité de certification est un prestataire qui produit des certificats, pour le compte d'utilisateurs.

L'autorité de certification signe le certificat (avec sa propre clé privée), garantissant ainsi l'intégrité du certificat et la véracité des informations contenues dans les certificats qu'elle émet.

L'autorité de certification assure le lien entre l'utilisateur (le futur signataire) et le certificat qu'elle va émettre pour lui, en s'assurant préalablement, par l'examen de pièces d'identité et le cas échéant, selon

le niveau de sécurité, par une rencontre en face-à-face, de la véracité des informations fournies par le demandeur du certificat.

3. Le certificat électronique qualifié est un document sous forme électronique

160

Le certificat électronique atteste du lien entre l'identité du signataire et les données de vérification de signature électronique. Il doit comporter :

- une mention indiquant qu'il est délivré à titre de certificat électronique qualifié ;
- l'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi ;
- le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
- le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
- les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
- l'indication du début et de la fin de la période de validité du certificat électronique ;
- le code d'identité du certificat électronique ;
- la signature électronique avancée du prestataire de service de certification électronique qui délivre le certificat électronique ;
- le cas échéant, les limites à l'utilisation du certificat électronique, et notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

D. Rôle du prestataire de service de certificat électronique

170

Le prestataire de service de certification électronique doit :

- faire preuve de la fiabilité des services de certification électronique qu'il fournit ;
- assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;
- assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;
- veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;
- employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;
- appliquer des procédures de sécurité appropriées ;
- utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;
- prendre toute disposition propre à prévenir la falsification des certificats électroniques ;
- dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;
- veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;
- conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.

- utiliser des systèmes de conservation des certificats électroniques garantissant que :

    1. l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire et que l'information puisse être contrôlée quant à son authenticité ;
    2. l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
    3. toute modification de nature à compromettre la sécurité du système peut être détectée ;

- vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;
- s'assurer au moment de la délivrance du certificat électronique que les informations qu'il contient sont exactes et que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;
- avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit, le cas échéant par voie électronique, la personne demandant la délivrance d'un certificat électronique :

    1. des modalités et des conditions d'utilisation du certificat ;
    2. du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique ;
    3. des modalités de contestation et de règlement des litiges ;

- fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au point précédent qui leur sont utiles.

180

Les prestataires de services de certification électroniques mentionnés au **I-D § 170** doivent être qualifiés dans les conditions prévues à l'article 7 du décret n° 2001-272 du 30 mars 2001 et selon les procédures prévues à l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

190

Le certificat électronique, qui contient les données de vérification de la signature électronique, doit être communiqué au destinataire des factures.

II. Factures électroniques assorties d'une signature électronique admise par l'administration comme équivalente à une signature " qualifiée "

200

Le référentiel général de sécurité (RGS) est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information destiné principalement, mais non exclusivement, aux autorités administratives qui proposent des services en ligne aux usagers.

210

Le signataire de la facture est celui qui détient et met en œuvre le moyen de signature. Il peut s'agir d'une personne morale (on parle alors « de cachet serveur ») auquel cas le cachet peut être produit automatiquement lors de l'envoi des factures, ou d'une personne physique (on parle alors de signature) émettant les factures après les avoir signées en son nom pour le compte de l'entreprise.

La signature ou le cachet serveur doit être lié au document de manière indéfectible.

220

Une signature électronique et un cachet serveur équivalant au moins au niveau deux étoiles du RGS permettent à eux seuls de garantir l'authenticité de l'origine et l'intégrité du contenu de la facture électronique. Aucune piste d'audit n'est nécessaire.

230

Pour être dispensé de piste d'audit, le dispositif de création de signature ou le dispositif de création de cachet serveur doit en outre être qualifié au sens du chapitre III du décret n° 2010-112 du 2 février 2010 afin d'attester de sa conformité à un niveau du RGS.

240

De plus, le certificat de signature ou le certificat de cachet serveur doit être délivré par un prestataire de service de certification électronique qualifié au sens du chapitre IV du décret n° 2010-112 du 2 février 2010.

La qualification d'un prestataire de service de confiance (PSCO) permet en effet d'attester de sa conformité à un niveau de sécurité du référentiel général de sécurité. Elle est délivrée par un organisme de qualification habilité par l'Agence nationale de sécurité des systèmes d'information (ANSSI). La liste des prestataires qualifiés est consultable sur le site de l'ANSSI dans la rubrique relative aux prestataires de service de confiance qualifiés.

III. Factures transmises par voie électronique et assorties d'une autre signature électronique

250

Les signatures électroniques autres que celles visées au I et II de la présente sous section garantissent l'authenticité de l'origine, l'intégrité du contenu et la lisibilité des factures seulement si elles s'accompagnent de la mise en place de contrôles établissant une piste d'audit fiable (BOI-TVA-DECLA-30-20-30-20).

Elles constituent un élément de la piste d'audit car elles permettent de détecter toute modification de la facture d'origine (condition d'intégrité).

260

Les signatures électroniques doivent au moins être « avancées » au sens de l’article 2 de la directive n° 1999/93/CE du 13 décembre 1999.

La signature électronique avancée peut être définie comme une donnée sous forme électronique qui est jointe ou liée logiquement à d’autres données électroniques et qui sert de méthode d’authentification du signataire et de l’origine des informations.

270

Elle doit ainsi satisfaire aux exigences suivantes :

- être propre au signataire ;
- permettre d'identifier le signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir le lien avec les factures auxquelles elle s'attache, de telle sorte que toute modification ultérieure de ces factures soit détectable.

280

Le signataire peut être une personne morale, auquel cas la signature électronique peut être produite automatiquement lors de l'envoi des factures, ou une personne physique émettant les factures après les avoir signées en son nom pour le compte de l'entreprise.

290

La signature électronique conforme au RGS une étoile peut aussi sécuriser les factures électroniques dès lors que des contrôles établissant une piste d'audit fiable sont mis en place dans l'entreprise.

Dans ce cas, il n'est pas nécessaire que le dispositif de création de signature ou le dispositif de création de cachet serveur ainsi que le prestataire de service de certification électronique soient qualifiés au sens du décret n° 2010-112 du 2 février 2010.

Les dispositions relatives au certificat électronique définies au I-C § 130 et suivants sont applicables au destinataire de factures électroniques assorties d'une signature électronique avancée ou conforme au RGS d'un niveau une étoile.

IV. Vérification de la signature électronique par le destinataire de la facture

300

Conformément à l'article 96 F bis de l'annexe III au CGI, l'entreprise destinataire de factures électroniques dont l'authenticité de l'origine et l'intégrité du contenu sont garantis au moyen d'une signature électronique dans les conditions prévues au 1° ou au 2° du VII de l'article 289 du CGI doit :

- vérifier la signature électronique apposée sur les factures au moyen des données de vérification contenues dans le certificat électronique ;
- s'assurer de l'authenticité et de la validité du certificat attaché à la signature électronique.

310

L'entreprise destinataire des factures doit, en effet, effectuer les vérifications relatives à l'authenticité et à l'intégrité du document, au moyen des données insérées dans le certificat électronique attaché à la signature électronique.

Cette vérification doit pouvoir être réalisée non seulement lors de la réception de la facture mais encore à tout moment pendant le délai de conservation prévu par l'article L. 102 B du livre des procédures fiscales (LPF).

La vérification de l’empreinte du document au moyen de la clé publique du signataire permet de s’assurer que le document signé par l’émetteur de la facture n’a pas été altéré ou modifié par la suite.

A cet égard, l’utilisation de fonctions macrodynamiques dans les fichiers factures doit être évitée. En effet, l’exécution de ces fonctions à chaque ouverture des fichiers en modifiera le contenu.

320

Par ailleurs, l’entreprise destinataire des factures doit également s’assurer de l’authenticité et de la validité du certificat électronique attaché à ces données de vérification de la signature électronique.

330

Ces dispositions sont applicables au destinataire de factures électroniques assorties d'une signature électronique (ou cachet serveur) quel que soit le format de cette dernière.