PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Signature électronique
Point de situation

MEMENTO

Version 0.94
25.08.04

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 41 46 37 20 - Fax 01 41 46 37 01

INTRODUCTION **3**

CONTEXTE JURIDIQUE **3**

DIRECTIVE EUROPEENNE 3
Objectif *3*
Effets juridiques de la signature électronique *3*
Initiative européenne de normalisation *4*
TRANSPOSITION FRANÇAISE 5
La modification du code civil *5*
Effets juridiques de la signature électronique *6*
Le décret 2001-272 du 30 mars 2001 ..... *6*

DISPOSITIF SECURISE DE CREATION DE SIGNATURE **7**

DEFINITION 7
SPECIFICATIONS TECHNIQUES 7
EVALUATION ET CERTIFICATION 8

CERTIFICAT QUALIFIE **9**

DEFINITIONS ET EXIGENCES POUR LE PRESTATAIRE 9
SCHEMA VOLONTAIRE DE QUALIFICATION 9
SPECIFICATIONS TECHNIQUES ET EVALUATION DES PRODUITS 11

EVOLUTION **11**

PUBLICATIONS DES NORMES 11
REVISION DE LA DIRECTIVE 11

ANNEXE 1 : SPECIFICATIONS TECHNIQUES **12**

ANNEXE 2 : NOTIONS JURIDIQUES **13**

NOTIONS SUR LA PREUVE EN DROIT FRANÇAIS 13
LA CONVENTION DE PREUVE 14
NOTION DE PRESOMPTION 14

Introduction

Ce document vise à dresser un point de situation sur la signature électronique dite « présumée fiable ». Partant d'un rappel sur le contexte juridique, il expose le cadre technique défini actuellement pour la mise en œuvre de ce type de signature.

Il est entendu que les lecteurs ont des connaissances minimales des outils techniques nécessaires à la mise en œuvre d'une signature électronique à l'aide de certificat (cf. FAQ sur les Infrastructures de Gestion de Clés).

Pour l'ensemble du vocabulaire utilisé dans ce document il est conseillé de se référer à la FAQ « Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ».

Contexte juridique

Ce chapitre donne l'historique des différentes étapes de la construction juridique du concept de signature électronique :

- la directive européenne,
- la transposition française.

Directive européenne

La directive du Parlement européen et du Conseil, du 13 décembre 1999, définit le cadre communautaire pour les signatures électroniques.

Objectif

Son objectif, rappelé dans l'article 1er de la directive, est de : «… *faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre pour les signatures et certains services de certification afin de garantir le bon fonctionnement du marché intérieur ».*

De plus : *« Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire ; elle ne porte pas non plus atteinte aux règles et limites régissant l'utilisation de documents, qui figurent dans la législation nationale ou communautaire.* »

Effets juridiques de la signature électronique

La directive reconnaît, dans son article 5, deux catégories de signature électronique, toutes deux recevables en justice, qui se distinguent par leurs exigences techniques et leurs effets juridiques.

Bas niveau de reconnaissance juridique

Une signature électronique, répondant à la définition qui en ait faite à l'article 2, ne pourra pas être refusée au titre de preuve en justice mais ne pourra prétendre à un niveau de reconnaissance équivalent à celui de la signature manuscrite.

« signature électronique », une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification. »

Haut niveau de reconnaissance juridique

Article 5.1 : « *Les **signatures électroniques avancées**, basées sur un **certificat qualifié**, et créées par un **dispositif sécurisé de création de signature** répondent 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 et soient recevables en justice.* »

L'équivalence de la signature électronique avec la signature manuscrite est acquise dès lors que trois conditions sont remplies :

- **la mise en œuvre d'une signature électronique avancée**, définie dans l'article 2 comme :

  « signature électronique avancée », une signature électronique qui satisfait aux exigences suivantes :
  a) être liée uniquement au signataire ;
  b) permettre d'identifier le signataire ;
  c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
  d) être liée aux données auxquelles elle se rapporte, de telle sorte que toute modification ultérieure des données soit détectable. »

- l'utilisation d'**un dispositif sécurisé de création de signature électronique**, certifié conforme aux exigences de l'annexe III de la directive (cf. article 3.4),

- l'utilisation d'**un certificat qualifié** pour vérifier la signature, c'est à dire : « *un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II » (cf. article 2).*

Initiative européenne de normalisation

A la suite de la directive européenne 1999/93/CE, la Commission européenne a lancé une initiative européenne de normalisation : EESSI (European Electronic Signature Standardization Initiative), afin de mettre sous formes de documents techniques normatifs les exigences retenues dans la directive et notamment celles figurant dans les annexes. Les travaux de normalisation ont été confiés à deux organismes européens :

- le CEN : Comité européen de normalisation,
- l'ETSI : European Telecommunications Standards Institute.

Conformément à la directive 1999/93/CE (article 3.4 et 3.5), la Commission européenne a publié le 15 juillet dernier au JOCE des références de normes, issues de cette initiative, après consultation du Comité article 9 (instauré par la Directive et composé de représentants des Etats membres). *(cf.* Publications des normes*)*

Transposition française

La transposition française s'est effectuée en plusieurs étapes par :

- **la loi n°2000-230 du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique,
- **la loi n°2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique, notamment son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés,
- **la loi n°2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui transpose, dans son article 5 l'article 8 de la directive, relatif à la protection des données (nouvel article 33 dans la loi du 6 janvier 1978 modifiée),
- **le décret n°2001-272 du 30 mars 2001**, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, modifié par le décret n°2002-535 du 18 avril 2002,
- **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,
- **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.

La modification du code civil

La modification principale est l'insertion de l'article **1316-4** dans le code civil par l'article 4 de la **loi n° 2000-230 du 13 mars 2000** parue au journal au journal officiel du 14 mars 2000. Cet article définit la signature et pose l'équivalence entre la signature électronique et la signature manuscrite sous certaines conditions.

Les réflexions, menées lors de la transposition de la directive 1999/93/CE en droit français, ont permis d'introduire dans le code civil une définition de la signature. Ainsi, le premier alinéa de l'article 1316-4 définit la signature comme suit : " *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte* ".

Le deuxième alinéa de l'article 1316-4 du code civil définit plus particulièrement la signature électronique, posant ainsi l'équivalence entre la signature électronique et la signature manuscrite sous certaines conditions :
« Lorsqu'elle [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».
Dés lors, toutes les signatures électroniques sont recevables en justice à partir du moment ou elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et la garantie de l'intégrité de l'acte signé.
Sous certaines condition, la fiabilité du procédé de signature électronique est présumée.
« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'Etat. » (article 1316-4 du Code civil)

Effets juridiques de la signature électronique

Cette loi esquisse donc deux niveaux de validité juridique pour les signatures électroniques dont les caractéristiques sont définies dans le décret 2001-272 du 30 mars 2001

- la signature électronique « simple »,
- la signature électronique « présumée fiable ».

La signature électronique « simple »

L'article 4 de la loi 2000-230 du 13 mars 2000 définit la signature électronique en ces termes :
« *Lorsqu'elle [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».*
A ce niveau, le procédé de signature électronique n'est pas présumé fiable mais l'écrit signé ainsi sous forme électronique ne pourra être refusé en justice au titre de preuve dès lors que le procédé permet d'identifier le signataire et de garantir le lien avec l'acte signé. En cas de contestation, il est nécessaire de prouver la fiabilité du procédé de signature électronique utilisé.

La signature électronique « présumée fiable »

L'article 4 de la loi 2000-230 du 13 mars 2000 précise que la charge de la preuve peut être inversée, en cas de contestation, sous certaines conditions définies par décret :
« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'Etat. »

Le décret 2001-272 du 30 mars 2001

L'article 2 du décret 2001-272 du 30 mars 2001 décrit les conditions selon lesquelles le procédé de signature électronique est considéré comme fiable :

- la **signature électronique est sécurisée** : c'est à dire qu'il s'agit d'une donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache et qui satisfait, en outre, aux exigences suivantes :
    - être propre au signataire ;
    - être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
    - garantir, avec l'acte auquel elle s'attache, un lien tel que toute modification ultérieure de l'acte soit détectable.

- la signature électronique est établie grâce à un **dispositif sécurisé de création de signature électronique.** Pour qu'un dispositif de création de signature soit reconnu comme sécurisé, il doit répondre à un certain nombre d'exigences décrites dans l'article 3.I du décret 2001-272 et être certifié conforme à ces exigences,

- la vérification de la signature électronique repose sur l'utilisation **d'un certificat électronique qualifié :** article 6 du décret.

Pour bénéficier de la présomption de fiabilité, le signataire devra donc mettre en œuvre une signature sécurisée utilisant un :

- Dispositif sécurisé de création de signature,

- et un Certificat qualifié.

Dispositif sécurisé de création de signature

Définition

La notion de dispositif sécurisé de création de signature englobe le procédé de génération du bi-clé de signature et sa mise en oeuvre pour signer un condensat de document.

L'annexe III de la directive définit les exigences pour un tel dispositif. Ces exigences sont reprises dans l'article 3.I du décret 2001-272 du 30 mars 2001 :

« *Un dispositif sécurisé de création de signature électronique doit :*

1) *Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :*

   a) *Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;*

   b) *Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;*

   c) *Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.*

2) *N'entraîner aucune altération du contenu à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.* »

Spécifications techniques

Le document **CWA 14169**, produit par le CEN, est écrit sous la forme de trois profils de protection (présentés respectivement dans les annexes A, B et C) correspondant à trois types de dispositifs de création de signature électronique différents :

- **PP SSCD type 1** : la cible d'évaluation de l'annexe A correspond au dispositif qui génère les données de création de signature électronique et de vérification de signature électronique,
- **PP SSCD type 2** : la cible d'évaluation de l'annexe B correspond au dispositif qui crée la signature électronique à partir des données de création de signature électronique et des données à signer,
- **PP SSCD type 3** : la cible d'évaluation de l'annexe C regroupe les deux fonctions précédentes : générer les données de création de signature électronique et de vérification de signature électronique et créer la signature électronique à partir des données de création de signature électronique et des données à signer.

Lorsque les données de création de signature électronique et de vérification de signature électronique sont générées par le prestataire de service de certification, le module cryptographique qu'il utilise doit être évalué et certifié. La spécification technique **CWA 14167-3** peut être utilisée à cet effet.

Des profils ou cibles de protection, autres que ceux définis sous l'égide de l'EESSI, peuvent être utilisés, à condition qu'ils couvrent complètement les exigences de la directive et du décret. En vue de l'attribution du certificat de conformité, ils doivent être acceptés au préalable par la DCSSI ou un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

D'autre part, l'EESSI a produit un document [**ALGO**] (Cf. Annexe 1) sur les algorithmes recommandés pour la signature électronique. Il s'agit d'un guide qui :

- liste les algorithmes acceptables pour la signature électronique et la taille minimale des clés pour ces algorithmes,
- prévoit une limite à la validité dans le temps des algorithmes recommandés.

Evaluation et certification

Pour bénéficier de la présomption de fiabilité du procédé de signature électronique, il est nécessaire entre autres que le dispositif de création de signature soit certifié.

L'article 3.II du décret 2001-272 du 30 mars 2001 précise les conditions suivant lesquelles le dispositif de création de signature électronique est certifié conforme aux exigences de l'article 3.I en ces termes :

« Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :

1° Soit par le Premier ministre, 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 est rendue publique ;

2° Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne. »

Le décret n°2002-535 du 18 avril 2002, relatif au schéma d'évaluation et de certification, a renforcé les bases juridiques du schéma français de certification qui reposait jusqu'ici sur un avis du Premier ministre de 1995. Il complète également le décret de signature électronique du 30 mars 2001, en fixant les règles de certification des produits de sécurité et notamment des dispositifs sécurisés de création de signature.

En se plaçant dans le cadre du décret 2002-535, l'évaluation du dispositif à certifier doit avoir lieu dans un centre d'évaluation agréé par la DCSSI. Ces centres d'évaluation réalisent des évaluations suivant des critères normalisés : les ITSEC (de moins en moins utilisés) ou la norme IS 15408 (aussi appelée "Critères Communs" (CC)). L'évaluation permet de certifier la conformité d'un dispositif à une cible de sécurité qui peut être conforme à un profil de protection.
L'évaluation, préalable à la délivrance d'un certificat de conformité au décret, doit s'appuyer sur une cible de sécurité qui couvre complètement les exigences du décret 2001-272 (article 3.I) et dont le niveau d'assurance est acceptable en fonction de l'environnement choisi.

Pour couvrir les exigences de l'article 3.I du décret énoncées plus haut (Définition), un dispositif sécurisé de création de signature électronique complet doit assurer au minimum les fonctions suivantes:

- la génération des données de création (clé secrète) et de vérification (clé publique) de signature électronique,
- la création de la signature électronique.

Chacune de ces fonctions peut être réalisée par un module distinct et faire l'objet d'un certificat de conformité.

Les produits évalués en vue d'une attribution d'un certificat de conformité au décret devront par ailleurs être soumis à une analyse des mécanismes cryptographiques qu'ils utilisent. Cette analyse est réalisée par la DCSSI.

L'attribution du certificat de conformité pour le dispositif sécurisé de création de signature électronique fait l'objet d'une procédure spécifique du schéma français de certification : SIG-P-01 Certification de conformité des dispositifs de création de signature électronique.doc

Certificat qualifié

Définitions et exigences pour le prestataire

Un certificat est reconnu comme qualifié s'il est conforme aux exigences de l'article 6.I du décret (transposition de l'annexe I de la directive) et s'il est fourni par un prestataire de service de certification électronique qui répond aux exigences définies dans l'article 6.II du décret (transposition de l'annexe II de la directive).

Il est à noter qu'un prestataire de service de certification, s'il considère qu'il satisfait aux exigences de l'article 6 du décret, peut déclarer délivrer des certificats qualifiés. Dans ce cas, comme indiqué dans l'article 9 du décret, il devra l'indiquer lorsqu'il se déclarera auprès de la DCSSI aux titres de la déclaration de fourniture de prestations de cryptologie effectuée conformément à l'article 28 de la loi du 29 décembre 1990.

En tout état de cause, les prestataires de service de certification déclarant délivrer des certificats qualifiés peuvent être contrôlés, conformément à l'article 9.II du décret : *« le contrôle des prestataires visés au I est effectué par la Direction centrale de la sécurité des systèmes d'information. Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique. ».* Si le contrôle n'est pas satisfaisant, la DCSSI assure la publicité des résultats du contrôle effectué.

Le décret, dans son article 8, prévoit également les règles de reconnaissance des certificats électroniques qualifiés fournis par des prestataires de certification électronique établis dans un pays tiers en dehors de la Communauté européenne.

Schéma volontaire de qualification

Les prestataires de service de certification (PSC) peuvent se soumettre volontairement à une évaluation pour être qualifiés (transposition de l'adjectif « accrédité » utilisé dans la

directive). Les certificats qu'ils délivrent sont alors présumés qualifiés. L'article 7 du décret 2001-272 du 30 mars 2001 spécifie que :

« Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés. »

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, annoncé dans le décret 2001-272 du 30 mars 2001 relatif à la signature électronique, définit le schéma français de qualification des PSC. Il est nécessaire de rappeler que les PSC se soumettent volontairement à ce type d'évaluation afin de se faire délivrer une attestation de qualification. Un prestataire sans attestation de qualification peut toutefois déclarer délivrer des certificats qualifiés s'il estime qu'il respecte les exigences de l'article 6 du décret.

En France, c'est le COFRAC qui est chargé d'accréditer les organismes qui procèderont à l'évaluation des prestataires de services de certification en vue de reconnaître leur qualification. Les organismes chargés de l'évaluation peuvent également se faire accréditer par des centres d'accréditation signataires de l'accord européen multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation. Le prestataire de service de certification choisit un organisme accrédité pour procéder à l'évaluation des services qu'il propose, et ce à ses frais.

L'évaluation, qui précède l'attribution de l'attestation de qualification, doit permettre de vérifier que le prestataire de service de certification respecte en tout point les exigences de l'article 6 du décret 2001-272.

A l'issue de l'évaluation, et en cas de réussite, une attestation de qualification est délivrée par l'organisme accrédité sur la base du rapport d'évaluation réalisé.

Le référentiel qui permet aux organismes accrédités de mener à bien leur évaluation est publié en annexe de cet arrêté.

Spécifications techniques et évaluation des produits

Les prestataires de service de certification doivent « *utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent* » (article 6.II.g du décret 2001-272). Les fonctions principales sont la génération et le stockage des clés du PSC et la signature des certificats qu'il émet.

Afin de traduire techniquement cette exigence (transposée de l'exigence f de l'annexe II de la directive), le CEN a produit une spécification technique, le **CWA 14167-2**, sous forme de profil de protection, qui couvre les fonctions mentionnées plus haut.
S'il demande à être qualifié ou pour garantir la qualité des produits et systèmes qu'il utilise, le prestataire pourra être amené à vouloir utiliser des produits certifiés conforme à ce profil de protection.

D'autre part, si le PSC génère également les clés de l'utilisateur, il devra utiliser un produit évalué et certifié. Il pourra pour ce faire utiliser le profil de protection issu de la spécification technique **CWA 14167-3**.

La DCSSI possède également un ensemble de profils de protection sur les IGC (PP_AC, PP_AE et PP_IGC) dont le **PP_RCIGC** (Profil de Protection Ressources Cryptographiques pour une Infrastructure de Gestion de Clés v 2.6, PPnc/0003) qui traite des fonctions de génération des bi-clefs pour le PSC (et éventuellement des bi-clefs des utilisateurs), ainsi que des fonctions de signature du PSC (certificat,…).

Evolution

Publications des normes

La Commission, après avis du Comité article 9 mis en place par la directive, a publié dans une décision en date du 14 juillet 2003, des références de normes s'appliquant d'une part aux dispositifs de création de signature électronique et d'autre part, aux modules cryptographiques utilisés par les prestataires de service de certification.
Un produit évalué et certifié conforme à une norme référencée dans la décision de la Commission sera alors présumé conforme aux exigences de la Directive et du décret correspondant :

- l'annexe III de la directive et l'article 3.I du décret 2001-272 pour le dispositif de création de signature électronique : référencement du CWA 14169,
- l'annexe II.f de la directive et l'article 6.II.g du décret 2001-272 pour le module cryptographique utilisé par le prestataire de service de certification : référencement des CWA 14167-1 et 1467-2.

Révision de la directive

La directive pourrait entrer dans un processus de révision. Cependant, aujourd'hui, nul ne connaît la portée des éventuelles modifications. De même, sa transposition en sera peut être impactée.

Annexe 1 : Spécifications techniques

Ci-dessous se trouve la liste des documents de spécification édités par le CEN/ISSS pour la signature électronique :

[ALGO]: ETSI SR 002176 Algorithms and Parameters for Secure Electronic Signatures v2.1 (19 Octobre 2001)

Guidelines for the implementation of SSCD PPs	CWA 14355
Guidelines for on the use of electronic signatures	CWA 14365
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures	CWA 14167-1
Cryptographic Modules for CSP Signing Operations – PP	CWA 14167-2
Secure Signature Creation Devices PPs	CWA 14169
Security Requirements for Signature Creation Systems	CWA 14170
Procedures for Electronic Signature Verification	CWA 14171
EESSI Conformity Assessment Guidance General	CWA 14172-1
EESSI Conformity Assessment Guidance Certification Authority services and processes	CWA 14172-2
EESSI Conformity Assessment Guidance Trustworthy systems managing certificates for electronic signatures	CWA 14172-3
EESSI Conformity Assessment Guidance Signature creation application and procedures for electronic signature verification	CWA 14172-4
EESSI Conformity Assessment Guidance Secure signature creation devices	CWA 14172-5

Ci-dessous se trouve la liste des documents de spécification édités par l'ETSI pour la signature électronique :

Policy requirements for certification authorities issuing public key certificates	TS 102 042
XML Advanced Electronic Signatures (XadES)	TS 101 903
XML format for signature policies	TR 102 038
Harmonised Trust Service Provider status information	TS 102 231
Qualified certificate profile	TS 101 862
Policy requirements for certification authorities issuing qualified certificates	TS 101 456
Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates	TS 102 158
Electronic Signature Formats	TS 101 733

Annexe 2 : Notions juridiques

Notions sur la preuve en droit français

Le système juridique français distingue la preuve des actes juridiques de la preuve des faits juridiques. Si la preuve des faits juridiques est libre, la preuve des actes juridiques est réglementée.

L'acte juridique est une « *opération juridique consistant en une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique* »[1]. Ainsi en est-il d'un contrat par exemple, qui va faire naître des obligations.
Par principe, le droit français n'est pas un droit formaliste, ce qui signifie que, dans un grand nombre de cas, aucune forme particulière n'est exigée pour qu'un acte juridique soit valable et produise des effets légaux. A ce titre, les contrats sont – par principe – valables quelle que soit la forme qu'ils peuvent revêtir (contrat oral, ...). On recourt cependant généralement à l'établissement d'une forme particulière, comme l'écrit, en vue de prouver l'existence de l'acte. En effet, même si le contrat oral peut être valable, il n'en reste pas moins difficile de prouver son existence.
Par exception, le droit impose le respect de certaines formes spécifiques, à défaut desquelles, la validité de l'acte pourra être remise en question. Le formalisme a pour avantage d'inviter les parties à la réflexion et à la vigilance sur l'importance et la portée de leur engagement, c'est pourquoi il est généralement imposé pour les actes qui peuvent avoir des conséquences importantes (ex. : contrat de cautionnement, …).

La formalisation des actes juridiques peut donc être établie à des fins de validité (*ad validitatem*) ou à des fins de preuve (*ad probationem*).

Dans les termes de l'article 1316-1 du Code civil, « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».
La validité des actes juridiques établis sous forme électronique est, quant à elle, soumise à un régime particulier (cf. la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).

Le présent mémento traite de la signature électronique des actes juridiques établis à des fins de preuve.

A la différence de l'acte juridique, le fait juridique est un *« fait quelconque auquel la loi attache une conséquence juridique qui n'a pas été nécessairement recherchée par l'auteur du fait* »[2]. La preuve des faits juridiques est libre. Il peut s'agir de présomptions, témoignages, aveux, serments, etc..

[1] G. Cornu, Vocabulaire juridique, Association H. Capitant, éd. PUF, 2001.
[2] G. Cornu, précité.

La convention de preuve

Les parties peuvent s'accorder conventionnellement pour reconnaître une valeur probante a certains éléments de leur relation contractuelle. Ces conventions de preuve sont valables dans certaines limites (ex : clause abusive). En pratique, l'utilisation de la convention de preuve est fréquente, particulièrement en matière d'informatique ou de télécommunications (ex : monde bancaire).

Notion de présomption

La présomption permet de bénéficier de conséquences juridiques sous réserve que certaines conditions soient remplies.
Ainsi, le décret 2001-272 du 30 mars 2001 a recours à deux reprises à la notion de présomption :

- article 2 : présomption de fiabilité du procédé de signature électronique :
  Un procédé de signature électronique sera considéré comme fiable par le juge en cas de litige si trois conditions sont remplies :
  - la signature créée répond à la définition d'une signature sécurisée au sens de l'article 1 du décret,
  - le dispositif de création de signature a reçu un certificat de conformité aux exigences de l'article 3.I du décret et dans les conditions énoncées dans l'article 3.II du décret,
  - le certificat électronique utilisé pour vérifier la signature comporte les champs énoncés dans l'article 6.I du décret et a été émis par un prestataire de service de certification respectant les exigences de l'article 6.II du décret.
- article 7 : présomption de conformité des certificats électroniques aux exigences de l'article 6 :
  - Un certificat électronique est considéré remplir l'ensemble des exigences de l'article 6 du décret s'il a été émis par un prestataire de service de certification qualifié.

Dans ces deux cas, il s'agit d'une présomption simple qui peut être renversée en apportant la preuve contraire.