Nos experts ont la parole
Utilisation juridique des documents

Denis Jacopini

Denis Jacopini est consultant en sécurité informatique et protection des données personnelles. Il nous propose d'aborder cette semaine «l'utilisation juridique des documents numériques à l'heure de la dématérialisation à outrance.»

«Dans le doute, après avoir numérisé un document officiel, vous avez probablement préféré conserver l'original dans son format matériel (bien souvent papier). A l'heure de la dématérialisation à outrance (remplacement dans une entreprise ou une organisation de ses supports d'informations matériels, souvent en papier, par des fichiers informatiques et des ordinateurs, jusqu'à la création de « bureau sans papier » ou « zéro papier » quand la substitution est complète), il est temps de se poser des questions sur la valeur juridique des documents informatiques en cas de contestation ou de litige. Le traitement de documents dématérialisés présente un certain nombre d'avantages significatifs.»

Transparence

«La dématérialisation garantit une plus grande transparence des procédures et une efficacité économique accrue. Traçabilité : La dématérialisation permet de conserver un historique de la réception des plis et de l'ensemble des échanges lors de la procédure. Cet historique, généré automatiquement par la plateforme de dématérialisation, a valeur de force probante.»

Economie de temps

«Les formulaires électroniques sont téléchargés sur Internet, ils sont préremplis et réutilisables. Les temps d'envoi des plis de réponse sont raccourcis, plus besoin de passer par un coursier ou de supporter les délais postaux, notamment les délais de retour des accusés de réception.»

Economie d'argent, d'espace

«Les frais d'impression des dossiers de réponse représentent des coûts non négligeables, d'autant plus qu'il s'agit généralement de plis volumineux. Les frais d'envois par courrier recommandé ou par coursier sont particulièrement lourds, un recommandé électronique possède la même valeur légale qu'un recommandé papier. L'archivage des pièces électroniques est plus simple et surtout moins consommateur d'espace.»

La preuve électronique

«Pour qu'un document électronique puisse être juridiquement utilisé et puisse constituer une preuve, on doit pouvoir au moins : Identifier l'auteur du document (ou de la signature), pouvoir affirmer qu'il est bien conforme à l'original (intégrité conservée). Pour atteindre ces objectifs, un système existe. Il s'appuie sur la notion de signature électronique.»

Signature électronique et valeur juridique

«La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La loi n° 2000-230 du 13 mars 2000 et son décret d'application du 30 mars 2001, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, a reconnu l'existence de la signature électronique sécurisée selon des critères stricts. Elle précise que toutes les signatures électroniques sont recevables en justice dès lors qu'elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et l'intégrité de l'acte.»

L'article 1316-4 du Code Civil

«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. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.»

«Il existe deux types de signatures électroniques : La signature électronique simple qui doit permettre d'apporter : l'authentification de l'auteur de l'acte, l'intégrité du message, la non répudiation de l'acte, la confidentialité du message (facultatif). Cette signature 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. Ce 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 sécurisée

«La signature électronique sécurisée/qualifiée présumée fiable qui en plus : est liée uniquement au signataire, permettre d'identifier le signataire, est créée par des moyens que le signataire peut garder sous son contrôle exclusif, est liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Seule la signature électronique sécurisée/qualifiée bénéficie de la présomption de fiabilité (article 2 du décret 2001-272). La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié. « 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'État.» La signature électronique est aujourd'hui le seul procédé informatique permettant de donner la même valeur juridique à un écrit électronique qu'à un écrit traditionnellement papier. »

Procédés cryptographiques

«La signature électronique n'est pas simplement l'apposition d'une image numérisée de la signature manuscrite sur un document numérique, elle consiste en l'usage de procédés cryptographiques permettant de faire le lien entre l'identité du signataire et le contenu du document et de le rendre intègre, pour interdire sa falsification ultérieure. Concrètement, pour qu'un document soit signé électroniquement (un courrier, une facture, un e-mail, une photo, une numérisation) et considéré conforme à l'original avec un auteur identifié il faut :

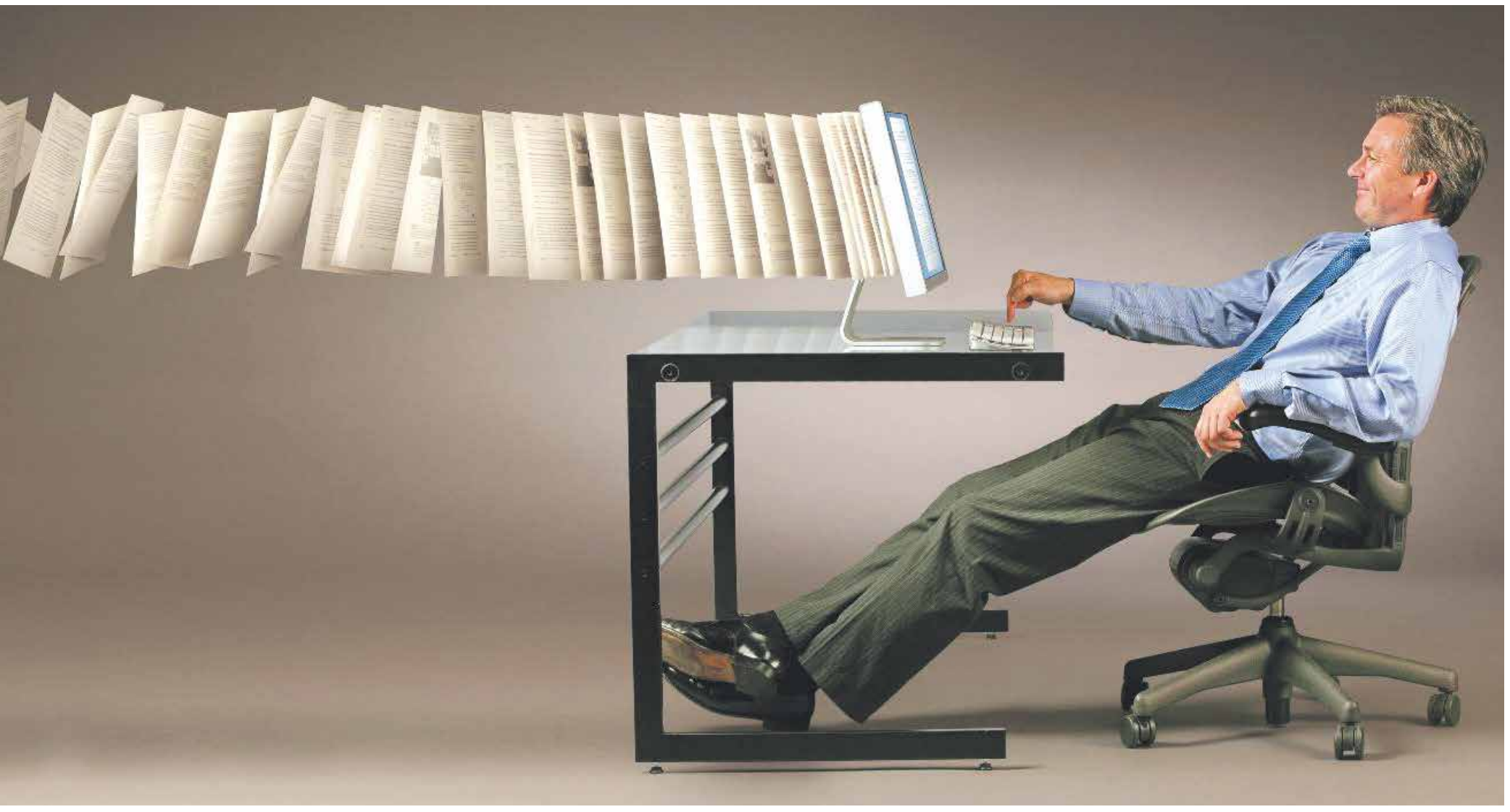
- Un certificat (c'est un fichier informatique attestant du lien entre les données de vérification de signature électronique et un signataire) ;
- Le certificat, qui représente votre identité numérique, est un fichier informatique qui associe vos données d'identification physiques à un résultat mathématique infalsifiable. Selon les niveaux de sécurité choisis, ce fichier, votre signature

Le net expert

Denis Jacopini est le fondateur de Le net expert. Il est expert judiciaire en informatique, diplômé en droit de l'expertise judiciaire, spécialisé en sécurité informatique, en informatique légale, en protection des données personnelles (Loi informatique et libertés et Cnil :), consultant en entreprises et collectivités territoriales. Le Net Expert propose un accompagnement dans deux principaux domaines : La mise en conformité de sites Internet et Système informatique par rapport à la Cnil et la Loi informatique et libertés. Le contrôle de la sécurité des données (contre la perte et contre la fuite) et des systèmes d'informations. Denis Jacopini collabore également avec la Web Osmose radio.

l'écho du mardi **Les Petites affiches de Vaucluse** n°3614 du 12 août 2014

numériques



électronique, sera soit sauvegardé dans l'ordinateur, soit mis sur une clé USB protégée ou bien mis sur une carte à puce et sera ensuite apposé sur les documents à signer.
Il existe quatre classes de certificat électronique : Classe I (équivalent au RGS zéro étoile).
Ne garantit pas l'identité du titulaire du certificat mais seulement l'existence de son adresse e-mail. Classe II (équivalent au RGS *) Garantit les informations du titulaire et de son entreprise (contrôlées par l'autorité de certification sur pièces justificatives transmises par voie postale). Classe III (équivalent au RGS **). Idem à la Classe II, assure un contrôle supplémentaire de l'identité du titulaire. Classe IIIPlus (équivalent au RGS ***)
Le RGS *** impose que le certificat soit remis en face à face sur un matériel certifié conforme au décret 2001-272. Remarque : La notion d'étoiles (*, **, ***) provient du décret Référentiel Général de Sécurité, qui, même s'il ne s'applique strictement qu'aux échanges entre les autorités administratives et leurs destinataires, constitue une échelle de valeur pour le marché français.»

Un dispositif de création de document électronique sécurisé

«Ce dispositif va avoir pour conséquence d'intégrer le certificat qui contient votre signature, dans le document original et d'en sortir un nouveau document dont l'auteur a été identifié, le contenu fixé ne pouvant plus être modifié sans s'en apercevoir et pouvant facultativement être rendu confidentiel et rendu lisible qu'à un seul destinataire). Si ce dispositif est sécurisé et donc conforme au 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, il sera considéré conforme aux exigences d'une signature présumée fiable.»

Identité du signataire

«Pour faire le lien entre l'identité du signataire et le contenu du document, et rendre tout intègre pour interdire sa falsification ultérieure, la seule technique existante à ce jour consiste en l'utilisation de deux outils informatiques : le certificat électronique délivré par une autorité de certification et l'application de signature électronique. Les certificats doivent être délivrés par des prestataires de services de certification électronique (PSCE) qualifiés. En France, c'est le Cofrac (Comité français d'accréditation) qui est chargé d'accréditer les organismes qui procéderont à l'évaluation des prestataires de services de certification en vue de reconnaître leur qualification.»

(plus d'informations sur http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1279.pdf)
La liste des PSCE (Prestataires de Services de Certification Electronique) qualifiés est consultable sur http://www.lsti-certification.fr/images/liste_entreprise/RGS.

La dématérialisation des factures

«Les entreprises souhaitant dématérialiser leurs factures, en format PDF, conformément à l'article 289-V du Code Général des Impôts, sont dans l'obligation de signer leur facture de façon électronique. En pratique, la signature est réalisée sur un serveur, sur lequel est installé le certificat électronique émis au nom de l'entreprise signataire. Remarque : Il est à noter que l'exigence du CGI relative à la signature électronique de factures, par une personne morale, est incohérente avec la notion de signature électronique, telle que définie dans le code civil, et visant généralement des personnes physiques. Cette disposition créé néanmoins un précédent intéressant sur lequel de nombreux usages, de signature de bulletins de paye, de contrats, s'appuient aujourd'hui.»

La dématérialisation pour les échanges avec le Service Public

«Depuis le 1er janvier 2005, les personnes publiques ne peuvent plus refuser la transmission des candidatures et des offres par voie électronique. Depuis le 1er janvier 2010, le pouvoir adjudicateur peut imposer la transmission électronique des documents et la transmission par voie électronique obligatoire pour les achats de fournitures de matériels informatiques et de services informatiques d'un montant supérieur à 90 000€ HT. Depuis le 1er janvier 2012 : le pouvoir adjudicateur ne peut plus refuser la transmission des documents par voie électronique pour les achats de fournitures, de services ou de travaux d'un montant supérieur à 90 000€ HT. Et enfin, depuis le 1er janvier 2014, L'UGAP (La centrale d'achat public), dans sa volonté d'accompagner cette évolution, signe de modernisation de l'achat public, a décidé d'imposer progressivement la réponse dématérialisée, à partir de mi-2012 en vue d'une généralisation de cette obligation à l'ensemble de ces secteurs. L'idée de cette obligation était d'encourager les entreprises à franchir le pas de la dématérialisation. Force est de constater qu'aujourd'hui, les sociétés et les collectivités ont encore des difficultés à appréhender les bénéfices qu'offre cette dématérialisation.

Nos experts ont la parole

Utilisation juridique des documents numériques (suite)

Cependant, au 1er Janvier 2015, toutes les structures devront dématérialiser leur comptabilité. En 2010, l'Anssi (l'Agence nationale de sécurité des systèmes d'information) a dévoilé un des moyens par lequel les services administratifs peuvent désormais sécuriser leurs procédures informatiques. Afin d'exposer le moins
possible les autorités aux risques de pertes de données, l'Anssi a souhaité mettre en place rapidement ce référentiel général de sécurité (RGS).» http://references.modernisation.gouv.fr/sites/default/files/DGME_Fiche_RGS_BAT.pdf

Les produits de sécurité qualifiée

«Les produits de sécurité qualifiée (protection en termes de confidentialité, intégrité, disponibilité, traçabilité ou authentification et en terme de sécurité : signature électronique, authentification, chiffrement, horodatage) doivent répondre aux exigences suivantes : à un besoin de l'administration. Les fonctions de sécurité qu'ils proposent sont conformes aux exigences du RGS de l'ANSSI (notamment en
matière de cryptographie). Ils ont fait l'objet d'une évaluation par un laboratoire spécialisé le CESTI (Centres d'Évaluation de la Sécurité des Technologies de l'Information). Remarque : Le recours à des produits qualifiés est la règle générale pour les administrations, les exceptions doivent être justifiées.»

Plusieurs niveaux de qualification

«Plusieurs niveaux de qualification (certification + besoin de l'administration) :

- qualification élémentaire : correspond à la CSPN (Certification de Sécurité de Premier Niveau) ;
- Qualification standard : analyse de la vulnérabilité du produit en fonction d'un potentiel d'attaque moyen. Correspond au niveau EAL 3+ (EAL = Evaluation Assurance Level voir tableau ci-dessous) selon les CC. (certification Critères Communs) ;
- Qualification renforcée : analyse de la vulnérabilité du produit en fonction d'un potentiel d'attaque élevé. Correspond au niveau EAL 4+ selon les CC. »

La dématérialisation pour les professions réglementées

«En plus d'utiliser des systèmes de certificat et de signatures électroniques, les ordres des différentes professions réglementées ont tous organisés l'échange numérisé de leurs membres à travers des réseaux sécurisés, souvent en mettant en place un VPN (abréviation : Virtual Private Network ou Réseau privé virtuel), ou en utilisant les standards de l'EDI (abréviation : Echanges de Données Electroniques). Il s'agit du RVPA pour les avocats, de télé@ctes pour les notaires, de InterAct par les huissiers de justice ou de RPVJ pour les juridictions civiles et pénales françaises depuis 2007 pour permettre la dématérialisation des procédures.»

La dématérialisation et la justice

«L'arrêté du 16 mai 2014 fixe la liste des cours d'appel participant à l'expérimentation prévue par le décret relatif aux frais et à l'expérimentation de la dématérialisation des mémoires de frais. Il s'agit des cours d'appel de Colmar, Metz et Rennes.»

Homologation des systèmes informatiques

«Lié à l'utilisation juridique des documents informatiques et dématérialisés, obligatoire pour les administrations et les services de l'État, l'homologation de son système d'information est une démarche aussi recommandée par l'ANSSI aux entreprises. (ANSSI : Agence nationale de la sécurité des systèmes d'information). Que ça soit pour garantir la protection des informations conformément à la réglementation, que ça soit pour être en mesure d'apporter la preuve que l'on a respecté la loi pour la protection des informations nominatives, classifiées de défense ou sensibles, que ça soit pour attester de son niveau de sécurité vis-à-vis de ses partenaires (Organismestiers, usagers, etc.) ou bien que ça soit pour mettre en place un SMSI (Système de Management de la Sécurité de l'Information) afin d'obtenir une vision cohérente en termes de place de la SSI dans le système d'information, de coûts, de priorités ou de responsabilités, tout système d'information des administrations et des services de l'État doivent faire l'objet d'une homologation de sécurité par une autorité d'homologation désignée par l'autorité administrative (RGS).»

Les étapes de l'homologation

« Les grands étapes d'une homologation d'un système informatique sont les suivantes :

- Identifier l'autorité d'homologation ;
- Obtenir une validation opérationnelle ;
- L'autorité d'homologation prononce une décision d'homologation ;
- Monter une commission d'homologation ;
- Bâtir le référentiel d'homologation et le valider en commission ; Auditer le système en fonction du référentiel ;
- Définir et mettre en avant les risques résiduels ;
- Homologuer le système au regard des risques résiduels. »

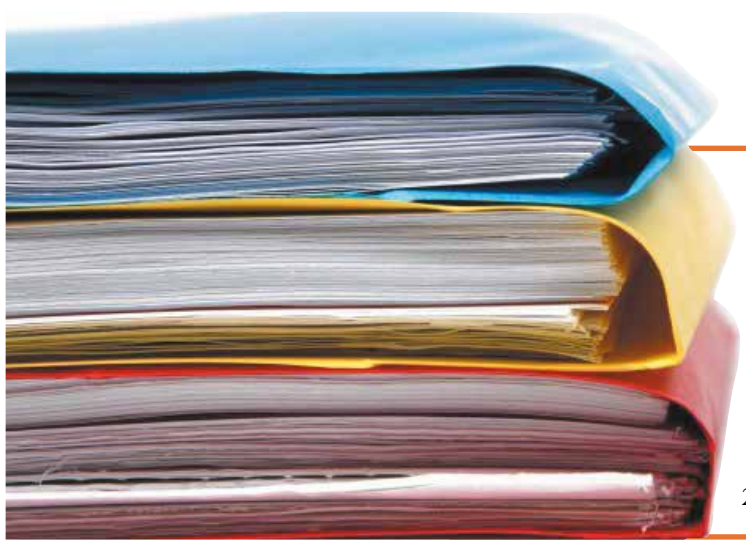
Les principaux acteurs

«Les principaux acteurs intervenants dans la démarche d'homologation : l'Autorité administrative ou l'Autorité Qualifiée responsable du système d'information et des informations qui y transitent ; l'Autorité d'homologation ou la personne désignée au sein de l'autorité administrative pour prononcer la décision d'homologation de sécurité du système d'information ; Le RSSI (Responsable de Sécurité des Systèmes d'Information) qui réalise l'analyse de risque et écrit les principaux livrables associés FEROS (Fiche d'expression rationnelle des objectifs de sécurité) ou PSSI (politique de sécurité des systèmes d'information) ; L'auditeur qui réalise l'audit de sécurité, pivot de l'homologation ; La Direction d'exploitation responsable de l'exploitation du système ; Le Maître d'oeuvre et maître d'ouvrage qui définissent et conçoivent le système. L'autorité administrative désigne une autorité d'homologation.»

Au terme de la procédure d'homologation

«Selon les résultats de l'analyse effectuée lors de la démarche d'homologation, l'autorité d'homologation pourra prononcer : une homologation provisoire, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ; une homologation, assortie le cas échéant de conditions, pour une durée déterminée (recommandée entre 3 et 5 ans) ; un refus d'homologation, si les résultats de l'audit font apparaître des risques résiduels jugés inacceptables. »

Denis Jacopini



Sources et Références

www.ssi.gouv.fr
www.ssi.gouv.fr/fr/reglementation-ssi/signature-electronique/qualification-des-prestataires-de-services-decertification-electronique-psce.html
www.lemoniteur.fr/165-commande-publique/article/actualite/22600295-la-dematerialisation-des-marchespublics-un-processus-qui-fait-debat
www.achats-publics.fr/Qui-Sommes-Nous/Dematerialisation.html
www.alpi40.fr/filemanager/download/111367/la_dematerialisation.pps
clubpsco.fr/wp-content/uploads/2012/07/GT-1-GT-Interop-Document-pedagogique-signature-electronique-20120627.pdf