Résumé

La 21CFR Part 11[1](souvent abrégée en 21CFR11) est un ensemble de dispositions réglementaires qui émanent de la FDA[2] et qui ont pour but de spécifier dans quelles conditions une organisation souhaitant satisfaire aux exigences de la FDA en matière de conservation des enregistrements et de soumission de l'information doit procéder aux enregistrements et signatures électroniques. La gestion des données est soumise à un certain nombre de règles destinées à offrir des garanties équivalentes de pérennité, d'authenticité, de confidentialité et de traçabilité, que l'on s'appuie sur des enregistrements électroniques ou papier. L'entrée en vigueur du texte date de 1997 ; son interprétation présentant une importante marge d'interprétation, il a été précisé depuis par de successifs guides de conformité 21CFR Part 11[3], sans qu'aucun n'offre d'éclaircissement définitif.

Ce texte, fondamental pour les entreprises désireuses de mettre sur le marché américain des produits soumis au contrôle de la FDA, demande donc à être compris et interprété par chaque organisation. On notera en effet que ce n'est pas un logiciel qui est conforme aux prescriptions de la FDA, mais l'application qui en est faite dans l'entreprise. Cependant, afin de faciliter les opérations de validation des systèmes informatiques par rapport aux exigences de la 21CFR Part 11, il est souvent souhaitable, lorsque l'on envisage l'acquisition d'un nouveau logiciel ayant pour vocation de gérer des données en liaison avec l'agrément FDA et plus largement avec la santé du consommateur ou patient, de mener une étude préalable de sa capacité à se conformer aux directives de la FDA.

ENNOV intègre, **de façon native**, des fonctionnalités facilitant les enregistrements et signatures électroniques sécurisés, ce qui fait que la mise en oeuvre des applications se révèle être de l'ordre du **paramétrage** et non pas du développement.

Le présent document reprend les différentes exigences de la 21CFR Part 11 et donne l'interprétation qui en est faite par ENNOV ainsi que les fonctionnalités correspondantes du logiciel.

---

[1] Partie 11 du chapitre (« Title ») 21 du « Code of Federal Regulation », intitulée « Electronic Records ; Electronic Signatures »

[2] Food and Drug Administration

[3] Le dernier guide de conformité (*Guidance for Industry – Part 11 : Electronic Records ; Electronic Signatures – Scope and Application*) a été diffusé en août 2003. Nous donnons ici une traduction libre de son introduction : « Ce guide a pour objectif de détailler la position actuelle de la FDA en ce qui concerne le champ d'application et la mise en oeuvre de la partie 11 du Chapitre 21 du Code of Federal Regulation ; Electronic Records ; Electronic Signatures.

Ce document fournit une ligne de conduite aux personnes qui, afin de satisfaire aux exigences relatives à la conservation des enregistrements ou à la soumission d'information à la FDA, exigences formulées par les statuts ou toute autre part de la réglementation FDA, ont choisi de conserver leurs enregistrements ou dossier de soumission de manière électronique, et se sont, de ce fait, soumises au respect de la partie 11. La partie 11 s'applique à tout enregistrement au format électronique qui serait créé, modifié, maintenu, archivé, retiré ou transmis au titre de l'un des enregistrements exigés par la réglementation de l'Agence. La partie 11 s'applique également aux enregistrements électroniques soumis à l'Agence au titre du Federal Food, Drug and Cosmetics Act (l'Acte) et du Public Health Service Act (l'Acte PHS), et ce bien que la réglementation de l'Agence ne fasse pas spécifiquement état de tels enregistrements (§11.1). »

I. Définitions

Agence

Il s'agit de la FDA. Les autres agences, l'AFSSAPS[4] pour la France, l'EMEA[5] pour l'Europe, élèvent leur niveau d'exigence et on peut s'attendre à une convergence des réglementations en matière de signature électronique.

Systèmes Clos / Ouverts :

- Systèmes Clos : les systèmes dont le client contrôle intégralement l'accès physique et logique (A.3.b.4)
- Systèmes Ouverts : les systèmes non clos (A.3.b.9)

On considère les systèmes externalisés pour tout ou partie comme des Systèmes Ouverts.

Biométrie (A.3.b.3)

Méthode de vérification de l'identité d'un individu basée sur la mesure d'une caractéristique physique propre et mesurable de l'individu.

Enregistrement électronique ou informatisé (A.3.b.6)

Toute donnée électronique créée, modifiée, conservée, archivée, récupérée ou diffusée par un système informatisé.

Système informatisé

Système électronique automatisé permettant de créer, modifier, conserver, maintenir, archiver, récupérer, restituer des enregistrements.

Signature Manuscrite (A.3.b.8)

Nom ou marque légale d'une personne sous forme de trace manuscrite ayant pour but d'authentifier un écrit de manière définitive.

Signature Électronique (A.3.b.7)

Ensemble de données (souvent un couple de clefs) validé adopté et autorisé par un individu constituant un engagement légal équivalent à sa signature manuscrite.

Signature Digitale ou Numérique (A.3.b.5)

Signature Électronique encodée avec des données d'enregistrement de manière à :

- Assurer l'identité du signataire,
- Donner un moyen de vérification de l'intégrité des données signées.

[4] Agence Française de Sécurité SAnitaire des Produits de Santé

[5] European MEdicines Agency

II. Champ d'application de la 21CFR Part 11

Enregistrements soumis à la réglementation

Les enregistrements électroniques soumis à la réglementation sont ceux qui sont :

- créés,
- modifiés,
- conservés,
- archivés,
- retirés,
- transmis

dans l'optique d'un dépôt à la FDA.

Cette partie ne s'applique pas aux enregistrements papier transmis par un moyen électronique, comme, par exemple, une télécopie.

Conditions d'acceptation

Si les enregistrements et signatures électroniques sont conformes à la réglementation 21CFR Part 11, la FDA les considère comme équivalents à leur version papier.

La FDA accepte les enregistrements électroniques satisfaisant le 21CFR11 à moins qu'elle ne requière expressément une version papier.

Le matériel, les logiciels, les données, les contrôles et la documentation du système doivent être disponibles pour une inspection de la FDA.

III. Principes généraux de l'implémentation par ENNOV

La signature

ENNOV redemande le code et le mot de passe, même pour une série de signatures consécutives.

Le logiciel enregistre en une seule fois:

- l'identification du signataire avec son nom complet,
- l'identification de l'objet signé,
- la signification de la signature (étape du workflow),
- l'horodatage de la signature.

La consultation (affichage, impression du document)

Le nom légal ou nom complet, les date et heure et signification de la signature en clair peuvent être présentées sur toutes les formes visibles de l'enregistrement (fiche signalétique, document de consultation).

L'horodatage (en heure locale et GMT) présente l'année sur 4 chiffres, le mois, le jour, l'heure, les minutes, les secondes.

La signification de la signature est:

- une étape d'un workflow de signature, par exemple l'approbation (ENNOVDoc),
- une étape d'un processus, par exemple la clôture d'une action corrective (ENNOVProcess).

Le contrôle du circuit et des acteurs impliqués

La solution ENNOV assure une circulation de l'information maîtrisée. Toute donnée (enregistrement, document, dossier) suit un circuit prédéfini, dont l'application garantit le déroulement conforme aux spécifications de l'organisation : étapes, dates butoir, acteurs autorisés sont définis.

La traçabilité

ENNOV garantit un enregistrement et une conservation des données conformes aux spécifications de l'organisation qui met en place l'outil. L'administrateur définit quels sont les informations dont la modification doit donner lieu à révision formelle du document, les étapes auxquelles cette modification est possible, ainsi que la conservation des anciens enregistrements. Ces fonctions sont natives dans la solution (ENNOVProcess, ENNOVDoc et ENNOVDossier).

Le module complémentaire 21CFR Part11 ajoute à ces fonctions natives l'enregistrement dans une base dite "audit trail" de toute modification intervenue sur n'importe quel champ de la base, en indiquant valeurs antérieure et postérieure au changement, date et heure du changement intervenu, et identité de l'acteur.

La gestion par entité

L'organisation d'une application ENNOV s'appuie sur la notion d'entité. Une entité correspond à un découpage logique en sous-ensembles de documents ou de processus obéissant à des règles de gestion communes et placés sous la responsabilité d'un même groupe d'administrateurs, par exemple des sites géographiques, des départements ou des systèmes de management.

Les fonctionnalités 21CFR Part11 ne sont pas indispensables pour tous les sites ou départements de l'entreprise.

C'est pourquoi l'activation des fonctionnalités du module ENNOV CFR21 peut être réalisée par entité, par exemple :

- l'audit trail,
- la double signature des documents,
- la double signature par étape de processus.

IV. Enregistrements et signatures électroniques

Cette partie analyse point à point la manière détaillée dont ENNOV répond aux exigences de la FDA en matière d'enregistrements électroniques.

Nota Bene : dans cette partie on trouvera :

- **dans la première colonne, précédée de sa référence dans la réglementation 21CFR11, la reprise textuelle de l'exigence énoncée par la FDA,**
- **dans la deuxième colonne, le mode de réponse à cette exigence :**
  - **P si elle doit être procédurée par l'entreprise,**
  - **S si le système doit l'assurer,**
- **dans la troisième colonne, l'interprétation synthétique que fait ENNOV de cette exigence,**
- **dans la quatrième colonne, la(les) fonctionnalité(s) d'ENNOV qui répondent à l'exigence,**
- **dans la cinquième colonne, la mention:**
  - **'O' pour "conforme",**
  - **'N' pour "non-conforme",**
  - **'N/A' pour "non applicable".**

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.a - Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	PS	Le système doit être validé en ce qui concerne sa capacité à détecter les enregistrements invalides ou altérés.	ENNOV répond à ces exigences en utilisant comme stockage une base de données relationnelle considérée nativement comme un “socle” conforme aux exigences de la FDA (par exemple l’environnement ORACLE ou Microsoft SQL Server).	O
B-11.10.b - The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records	S	Les enregistrements doivent être disponibles : • à l'écran, • ou sous forme papier, • ou sous forme électronique via un export pour l'auditeur FDA n’ayant sur son ordinateur que les outils bureautiques les plus courants. La FDA accepte les enregistrements au format PDF.	ENNOV offre la possibilité : • de rechercher les enregistrements (requêtes, plan de classement, ...), puis d'exporter les enregistrements électroniques complets dans un format CSV ou XML, • de générer des documents bureautiques convertis au format PDF contenant, intégrées au moyen de signets, les données des documents et des processus.	O
B-11.10.c - Protection of records to enable their accurate and ready retrieval throughout the records retention period.	PS	Les enregistrements doivent être protégés pendant la durée légale de rétention.	Le stockage des enregistrements (méta-données et documents).est réalisé dans une base de données hébergée sur un serveur sauvegardé selon les procédures du client.	O

[6] Responsabilité = (P)rocédure ou (S)ystème

[7] Conforme

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.d - Limiting system access to authorized individuals	PS	Le système doit être protégé contre l'accès de personnes non autorisées.	ENNOV s'appuie sur les mécanismes d'authentification de ses clients (NTLM, LDAP, Active Directory, Kerberos, SSO, …). Les règles de composition et durée de vie du mot de passe sont déléguées au système d'authentification du client. ENNOV enregistre les tentatives d'accès infructueuses et bloque le compte après un nombre, paramétrable, de tentatives infructueuses. Les profils d'utilisation de l'application sont clairement définis dans les utilitaires ENNOV et auditables par un intervenant extérieur. ENNOV est une application Web. Les sessions utilisateurs ont une durée de vie paramétrable, ce qui signifie qu'une page inactive pendant un temps paramétré devient inutilisable, ce qui oblige l'utilisateur à une nouvelle connexion.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.e - Use of secure, computer-generated, time stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	S	Ce point précise qu'il doit exister un horodatage des données ainsi qu'un audit trail sur toutes les actions faites par les opérateurs influençant les données enregistrées. On entend par audit trail un enregistrement de toutes les opérations effectuées dans la base de données. Le système doit comporter une fonction d'audit trail sécurisé de chaque enregistrement GMP[8] et des actions de l'opérateur. Cet audit trail doit être conservé aussi longtemps que les enregistrements auxquels il se rapporte. Il doit être disponible pour être inspecté ou externalisé pour l'agence.	L'audit trail d'ENNOV donne le nom de l'opérateur ayant fait l'action, l'action effectuée, le motif (action, vérification, approbation, ...), la date et l'heure locale et GMT. Une fois une ligne ajoutée au fichier d'audit trail, elle ne peut pas être modifiée ni supprimée. L' Audit Trail est créé de façon incrémentale, dans l'ordre chronologique, et de manière a ce qu'il soit impossible qu'une nouvelle information d' Audit Trail écrase une information existante. Les évènements systèmes donnant lieu à une inscription dans ce fichier sont : • Création d'un enregistrement, • Modification d'un enregistrement (dans ce cas les valeurs avant et après modification sont inscrites), • Suppression d'un enregistrement Le système comprend des fonctions permettant de réaliser des requêtes sur l'audit trail ceci afin d'avoir la possibilité de fournir les informations exactes souhaitées par l'Agence. Celles-ci sont exportables sur un PC standard aux formats CSV et XML. Les informations d'audit trail font partie des sauvegardes régulières puisqu'elles sont enregistrées dans la même base de données que les données vivantes.	O

[8] Good Manufacturing Practices

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.f - Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	PS	Le système doit être capable de contrôler, lorsque cela est approprié, le respect d'une séquence d'étapes ou d'opérations (Workflow)	C'est le principe de base d'ENNOV Process que d'automatiser un processus sous la forme d'un enchaînement d'étapes affectées à des acteurs selon des règles définies.	O
B-11.10.g -Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	PS	L'entreprise doit contrôler des interventions autorisées sur les enregistrements (création, modification, suppression). L'accès direct aux données stockées doit être contrôlé ainsi que les interventions directes sur le processus supervisé.	Seuls les individus autorisés ont accès au système avec des droits en accord avec leur profil. Le système propose des outils d'administration (utilitaires) pour allouer ou supprimer des droits d'accès à des processus, des enregistrements ou des actions.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.h - Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	PS	Il s'agit de sécuriser les actions de commandes opérateurs étape par étape (obligation de passer par certaines étapes) au cours de la supervision d'un processus (acquittement d'alarmes, démarrage de processus, correction de paramètres, lancement de rapport de fin de lot,....). Chaque action doit pouvoir être effectuée par le ou les seuls opérateurs habilités à la réaliser. Certaines de ces actions doivent même être vérifiées ou validées par une autre personne elle-même habilitée à le faire, le tout devant être tracé dans un audit trail (voir B-11.10.e). D'autre part, il est nécessaire d'enregistrer les tentatives infructueuses d'accès par un utilisateur non habilité.	ENNOV est capable de déterminer : • l'origine d'une entrée de données (nom de l'émetteur), • l'origine d'une instruction opérationnelle (traçabilité du processus). Les tentatives d'accès infructueuses sont enregistrées. Après un nombre de tentatives infructueuses paramétrable, le compte est bloqué et l'administrateur est informé par courriel du blocage. Seul l'administrateur peut débloquer le compte	O
B-11.10.i - Determination that persons who develop, maintain, or use electronic record systems have the education, training, and experience to perform their assigned tasks.	P	Les personnes qui développent et maintiennent (Ennov) ou utilisent le système doivent avoir la formation initiale, la formation continue et l'expérience nécessaire pour accomplir leurs tâches.	Le personnel d'Ennov possède la compétence requise pour développer, tester, former et accompagner les clients. Ennov est régulièrement auditée par ses clients. Ennov transfère la compétence sur le paramétrage et l'utilisation de ses produits aux clients.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.10.j - The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	PS	L'entreprise doit définir des politiques écrites et obtenir l'adhésion pour rendre les individus responsables et comptables des actions réalisées sous leur signature électronique de façon à décourager la falsification de la signature.	ENNOV permet de paramétrer la durée de vie d'une page de saisie. La double signature impose la connaissance du code et du mot de passe pour signer. Les règles de composition et de vieillissement du mot de passe sont déléguées au système d'authentification.	O
B-11.10.k - Use of appropriate controls over systems documentation including:		La documentation du système doit être contrôlée.		
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	P	La diffusion et l'accès à la documentation du système doivent faire l'objet de contrôles adéquats.	Le manuel utilisateur est livré au format PDF et accessible aux utilisateurs d'ENNOV.	O
(2) - Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	P	Le développement et la modification de la documentation du système sont conduits selon des procédures de révision et de maîtrise des changements qui comprennent un audit trail	Le système qualité d'Ennov est audité régulièrement par ses clients	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.30 - Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	S	L'accès à des systèmes ouverts doit inclure des mesures supplémentaires comme le cryptage ou la signature numérique.	Dans ce cas, une option permet de s'assurer de contrôles supplémentaires : • un système de cryptographie de bout en bout de la connexion, • une authentification forte par l'utilisation de certificats.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.50.a - Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	S	Les enregistrements électroniques signés doivent contenir le nom légal ou nom complet du signataire, les date et heure et signification de la signature en clair sur toutes les formes visibles de l'enregistrement.	L'horodatage (en heure GMT et heure locale) présente l'année sur 4 chiffres, le mois, le jour, l'heure, les minutes, les secondes. La signification est une étape d'un workflow de signature ou une étape d'un processus. Le nom complet du signataire apparaît dans la signature	O
B-11.50.b - The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	S	Les données du 11.50.a. doivent être traitées comme faisant partie intégrante de l'enregistrement et être présentés dans toutes les formes lisibles de l'enregistrement.	Ces données sont visualisables, imprimables et exportables avec les autres données de l'enregistrement. Dans ENNOVDoc, la signature est obligatoirement valide car elle est effectuée à un stade à partir duquel la modification est interdite. Dans ENNOVProcess, le paramétrage permet d'interdire la modification des données signées.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
B-11.70 - Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means	S	Le lien signature / enregistrement est impossible à distendre par un moyen courant.	La signature contient l'identification de l'enregistrement signé et la date de signature. Elle n'est donc plus valide si : • elle est associée à un autre enregistrement, • la date de signature est modifiée. Lorsque que le système imprime des données sur un document sur lequel figure la signature, ce document contient les informations adéquates permettant de déterminer avec certitude les enregistrements électroniques auxquels s'applique la signature.	O
C-11.100 a - Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	S	Une signature doit être : • personnelle, • unique pour chaque personne dans chaque système à un instant donné, • non réutilisable, • non ré-attribuable.	La gestion des mots de passe est déléguée au système d'identification du client.	O
C-11.100 b - Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	P	Vérification de l'identité des utilisateurs de la signature électronique.	Cette exigence concerne l'autorité de confiance qui délivre les clés numériques.	N/A

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
C-11.100 c - Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	P	L'engagement des utilisateurs et administrateur est réaffirmé dans le cas de la mise en place de signature électronique qui doit être reconnue par l'utilisateur comme l'équivalent de sa signature manuscrite dans un courrier (postal) adressé à la FDA.	Cette exigence s'applique au client.	N/A

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
C-11.200 a - Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	S	Pour les signatures non biométriques, le système doit utiliser au moins deux moyens d'identification distincts, tel qu'un code identifiant et un mot de passe, pour signer électroniquement. Lorsqu'un individu exécute une série de signatures durant une période continue d'accès contrôlé au système, le système peut autoriser cet individu à signer avec uniquement un composant de sa signature électronique, à condition que la première signature soit effectuée en utilisant tous les composants de la signature électronique. Le niveau de sécurité doit être tel que si une signature est réalisée par une personne non détentrice de cette signature cela signifie forcément que le détenteur a communiqué son mot de passe à quelqu'un. L'entreprise doit garantir à travers le système l'identité des personnes capables de signer électroniquement.	Les signataires doivent être répertoriés dans l'annuaire interne d'ENNOV. L'administrateur leur attribue un code. La gestion du mot de passe est déléguée au système d'authentification du client. En cas de série de signatures durant une période continue d'accès contrôlé au système, ENNOV demande les deux composants de la signature : le code et le mot de passe. Le droit de signer électroniquement est paramétré par l'administrateur, pour chaque couple entité/type de document.	O

Exigence 21CFR part 11	R[6]	Interprétation par Ennov	Fonctionnalité ENNOV	C[7]
C-11.200 b Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	PS	Le système doit être conçu pour garantir que les signatures électroniques basées sur la biométrie ne peuvent pas être utilisées par d'autres personnes que leur propriétaire.	Cette exigence s'applique au système d'identification biométrique interfacé avec ENNOV.	N/A

C-11.300 Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:				
C-11.300 a - Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	S	Le système doit être capable de maintenir l'unicité de chaque combinaison identifiant / mot de passe.	La gestion des mots de passe est déléguée au système d'identification du client.	N/A
C-11.300 b - Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	PS	La gestion des mots de passe liés à la signature doit respecter les critères de complexité, durée de vie, réinitialisation , de la procédure du client.	La gestion des mots de passe est déléguée au système d'identification du client.	N/A
C-11.300 c - Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	PS	Le système doit prévoir la possibilité de désactiver définitivement ou temporairement le procédé d'identification en place (carte ou token), en cas de perte. Le système doit prévoir la possibilité de fournir un procédé d'identification (carte ou token) de remplacement L'administrateur système peut révoquer une signature	Cette exigence concerne les signatures digitales sur carte à puce, clé USB ou système biométrique.	N/A

C-11.300 d - Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	S	Le système doit être capable de détecter et de tracer les tentatives d'utilisation non autorisées de signatures électroniques.	ENNOV enregistre les tentatives de signature erronées, incluant l'identité de l'utilisateur et l'horodatage de la tentative. Trois (paramétrable) tentatives de signatures échouées successivement désactivent la possibilité de signer. Seul l'administrateur peut débloquer le compte pour lui redonner la possibilité de signer. Le système est capable d'afficher ou de présenter sous forme électronique ou papier les informations du journal des tentatives d'accès. Le système alerte automatiquement, en utilisant la messagerie électronique, l'administrateur en cas de détection d'un échec répété de tentative de signature.	S
C-11.300 e - Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	P	Les équipements qui permettent de générer les codes ou mots de passe d'identification doivent être testés périodiquement.	Il s'agit de procédures client à mettre en place : • une validation du système doit être effectuée à la mise en service d'une carte ou token • une validation du système doit être effectuée au moins annuellement sur les cartes ou token	N/A

V. A propos d'ENNOV

ENNOV est une société d'édition de logiciel dédiée à la gestion des processus métiers et du cycle de vie des documents. ENNOV met au service de problématiques de Business Process Management des solutions novatrices, ouvertes, mariant rapidité de mise en place, souplesse et simplicité d'utilisation. Un simple navigateur, pas de formation pour l'utilisateur final : telle est notre philosophie de développement. Parmi nos clients Alstom, PSA, General Electric, Safran ou Veolia. ENNOV est une société française. Elle dispose d'un réseau de distribution sur l'Europe et les Etats-Unis.

ENNOV

251 rue du Fbg St Martin
75010 PARIS
ph. (33) 1 40388138
fax (33) 1 40388129

www.ennov.com