Niveaux de service d'archivage : Mise en place d'une FAQ

Le CFONB a publié en janvier 2010 un ensemble de documents conçus comme des aides à l'élaboration d'une politique d'archivage électronique au sein du monde bancaire.

Au sein de ce corpus documentaire, la brochure *« Niveaux de service d'archivage »* constitue un cahier des charges, élaboré selon la norme NF Z 042-13 publiée en mars 2009 par AFNOR. Elle précise les dispositions à retenir pour répondre aux divers degrés d'importance des documents à archiver, en ajoutant à la Conservation, des garanties de traçabilité, puis d'intégrité et enfin d'authenticité ».

Afin d'aider à la mise en œuvre de ces préconisations, une FAQ est présentée ci-après.

F.A.Q : Foire aux questions concernant le support «Niveaux de service d'archivage»

Septembre 2012

Id	Q/R	Texte
1	Question	Dans le paragraphe 4.1, il est défini comme un des principes applicables à tous les niveaux de service : *La journalisation conduit à la production d'attestations. Celles-ci doivent être archivées dans les mêmes conditions de conservation que les documents qu'elles concernent.* Cela veut-il dire que les attestations produites doivent être archivées en dehors du journal dont elles sont extraites ?
	Réponse	Oui, les attestations produites doivent être archivées indépendamment des journaux dont elles émanent.
2	Question	Dans le paragraphe 4.1, il est défini comme un des principes applicables à tous les niveaux de service : *Les journaux doivent être archivés selon une périodicité et des conditions définies par la politique d'archivage dans des volumes de stockage assurant au moins la même pérennité et intégrité que les documents auxquels ils se rapportent.* Pour le journal du cycle de vie, il est écrit pour le niveau 0 (paragraphes 4.2.2.1.2 et 4.2.2.1.3) : *Pas de condition particulière de conservation.* *Le journal doit faire l'objet d'une sauvegarde selon la politique de sauvegarde du système d'archivage électronique.* *La **conservation de ces traces** peut être limitée dans le temps, inférieure à la durée de l'archive.* *Le choix du **support de conservation** de ces traces est laissé à l'appréciation des établissements*. Pour le journal du cycle de vie, il est écrit pour le niveau 1 (paragraphes 4.2.2.2.2 et 4.2.2.2.3) : *Pas de sécurisation particulière en dehors des dispositifs pris par la politique de sécurité des établissements.* *Sa durée de conservation est compatible avec celle des archives.* Pour le journal du cycle de vie, il est écrit pour le niveau 2 (paragraphes 4.2.2.3.2 et 4.2.2.3.3) : *Une empreinte (hash) est calculée par journal, elle forme la première ligne du journal (principe du chaînage des journaux). La fin d'un journal doit comprendre la date de clôture de ce dernier.* *Chaque journal ainsi constitué sera archivé dans les mêmes conditions que les archives auxquelles il se rapporte. […]* A partir de quel niveau CFONB les journaux **doivent-ils** être archivés dans le SAE ?
	Réponse	Au niveau 0, les journaux sont sauvegardés pour une durée limitée définie par la politique de sauvegarde. A partir du niveau 1, les journaux sont archivés : ➔ Niveau 1 : la durée de conservation est compatible avec celles des archives ➔ Niveau 2 et 3 : Niveau 1 + empreinte et chainage Conclusion : L'archivage des journaux se fait à partir du niveau 1
3	Question	Il est écrit dans le paragraphe 4.2.1 :

Id	Q/R	Texte
		Le journal de cycle de vie des archives peut être global ou spécifique par entité gérée. 1 L'entité gérée peut-elle être une entité regroupant plusieurs documents ? 2 Les attestations étant des extraits du journal du cycle de vie, est-il acceptable qu'elles soient du même niveau que le journal, c'est-à-dire qu'elles concernent éventuellement un ensemble de documents ?
	Réponse	Voilà la lecture que le GT Archivage électronique fait de cet extrait de la norme NF Z 42-013 : 1/ Une entité est une entité organisationnelle ou juridique 2/ Les attestations portent sur les dépôts. Par exemple : - Si un dépôt est un dossier, alors l'attestation porte sur ce dossier ; - Si un dépôt est un document, alors l'attestation porte sur ce document.
4	Question	Il est écrit dans le paragraphe 4.2.1 : *Le journal de cycle de vie des archives comprend les attestations électroniques suivantes :* *1. attestation de prise en compte initiale d'un dépôt ;* *2. attestation de prise en compte d'une modification de la durée d'un dépôt, le cas échéant ;* *3. attestation de destruction anticipée ou à terme d'un dépôt, le cas échéant ;* *4. attestation de restitution d'un dépôt, le cas échéant ;* *5. attestation pour toute création, modification ou suppression d'un profil d'archivage.* Le terme « attestation électronique » doit-il être compris dans cette phrase comme une « trace électronique sur un événement » ?
	Réponse	Non, une trace électronique n'est pas une attestation. Toute production d'attestation est basée sur la mise en forme d'une trace électronique figurant dans le journal du cycle de vie des archives.
5	Question	Paragraphe 4.2.1 : *Le **journal de cycle de vie** des archives doit être mis à jour dès qu'une trace de création, modification ou suppression d'un profil d'archivage est générée ou qu'une nouvelle attestation électronique est générée.* Paragraphe 5.1.7 : *Seules les personnes dûment habilitées conformément à la politique de sécurité de l'établissement peuvent créer, modifier, ou supprimer un profil d'archivage.* *Chacune de ces actions doit faire l'objet d'une journalisation dans **le journal des évènements** du niveau de service correspondant.* 1 La création, modification, suppression d'un profil d'archivage est-elle tracée dans le journal du cycle de vie ou dans le journal des événements ? 2 Qu'entend-on exactement par création, modification, suppression d'un profil d'archivage : s'agit-il uniquement des informations de définition et de droits d'accès du profil, ou tout rattachement de groupe d'utilisateurs ou d'utilisateur au profil doit-il aussi être tracé ?
	Réponse	1/ La création, modification, suppression d'un profil d'archivage est tracée dans le journal du cycle de vie des archives – cf. paragraphe 5.2 de la NF Z 42.013 Profil d'archivage – bien que cela ne concerne pas une archive mais un profil d'archivage. 2/ Le point 5.1.7 mentionne une des exigences propre à la profession bancaire étant précisé qu'un profil d'archivage(1) n'est pas un profil d'accès, mais le regroupement des règles d'archivage applicables à une catégorie d'objets. *(1)Définition d'un profil d'archivage : voir NZ 42-013 paragraphe 3.26 page 11 -*
6	Question	Le paragraphe 4.2.2.1.1 définit ainsi le contenu du journal du cycle de vie de

Id	Q/R	Texte
		niveau 0 : *Dans ce niveau, seules des traces techniques sont écrites dans le journal. Il s'agit des opérations techniques nécessaires au suivi de l'application (pilotage), et qui permettent de détecter d'éventuels dysfonctionnements, l'acquittement des traitements d'archivage, et la suppression d'archives. Le niveau de détail de ces traces est variable, selon les établissements.* 1 Pourquoi les traces de pilotage de l'application ne figurent-elles pas plutôt dans le journal des événements (inexistant pour le niveau 0) ? 2 A quoi correspond l'acquittement des traitements d'archivage ? S'agit-il de l'événement de dépôt d'archive ? 3 Dans le paragraphe 5.1 (contrôles sur événements), les événements de dépôt et de suppression d'archive ne donnent lieu à aucun contrôle au niveau 0, pas même la journalisation. Doit-on donc tracer ou pas ces événements dans le journal du cycle de vie au niveau 0 ?
	Réponse	1/ Une question à préciser : Il semble être présupposé dans la question que les traces techniques sont des traces de pilotage du système, ce qui n'est pas toujours le cas, une trace technique peut être liée aux archives. 2/ Oui, il s'agit bien de l'événement de dépôt d'archive. 3/ Non, il n'y a pas de contrôle au niveau 0, donc pas de journalisation dans le journal du cycle de vie.
7	Question	Paragraphe 4.2.2.4.1 : *« Chaque attestation enregistrée dans le journal de cycle de vie des archives doit être signée par une UCA du système d'archivage de l'organisme, ou de l'entreprise, ou bien du tiers archiveur, au moyen d'une signature électronique. »* 1 Le terme « attestation » doit-il là encore être pris au sens « trace électronique sur un événement » ? (cf question 4) 2 Cela signifie-t-il que la signature électronique de chaque événement sur l'archive doit être conservée dans le journal du cycle de vie avec la trace de l'événement ? 3 Dans le paragraphe 5.1 (contrôles sur événements), pour le niveau 3, seuls les événements de dépôt, suppression et restitution d'archive sont soumis à un contrôle d'authentification par vérification de leur signature électronique. Confirmez-vous que les événements de lecture et de migration d'archive ne sont donc pas soumis à authentification par signature électronique pour le niveau 3 ? 4 Est-ce que le document déposé doit toujours être accompagné d'une signature électronique (en plus de la signature électronique de l'ordre de dépôt) ? Est-ce que la signature électronique du document déposé doit être consignée dans le journal du cycle de vie ? Est-ce que la signature électronique du document déposé doit être archivée dans le SAE ?
	Réponse	1/ Non, une trace électronique n'est pas une attestation Toute production d'attestation est basée sur une trace électronique figurant dans le journal du cycle de vie des archives. - cf. paragraphe 3.3 de la norme NF Z 42.013 : définition : ***« attestation électronique :*** *ensemble d'éléments permettant d'assurer qu'une action ou un échange électronique a bien eu lieu »-* 2/ Non, les traces des évènements dans le journal ne sont pas signées. Par contre, les attestations doivent être signées. 3/ Oui, le SAE ne contrôle pas sa propre signature. 4/ Au niveau 3, c'est l'archive (document ou dossier) qui est signée. Cette signature doit être archivée dans le SAE puisqu'elle fait partie de l'archive. Le contrôle de cette signature, comme le résultat du contrôle sont tracés dans le journal du cycle de vie.
8	Question	Dans le paragraphe 4.2.2.2.1 décrivant le contenu du journal du cycle de vie au

Id	Q/R	Texte
		niveau 1, il est écrit : *Lors de l'opération de dépôt, l'empreinte de l'objet archivé doit être consignée dans le journal si le support de stockage n'est pas de type WORM, elle servira notamment à vérifier l'intégrité de l'objet lors de sa consultation, ou de sa restitution.* *En cas de stockage sur un support WORM, l'intégrité est assurée par le support : pas de dispositif particulier au niveau du journal.* Pourtant, à ce niveau, il n'est pas prévu dans le paragraphe 5.1 (contrôles sur événements) la vérification de l'intégrité du document lors de la lecture ou de la restitution d'archive. 1 Doit-on vraiment, au niveau 1, conserver une empreinte du document dans le journal si le support n'est pas WORM ou cette préconisation est-elle valable seulement pour le niveau 2 voire le niveau 3 ? 2 Aux niveaux 2 (paragraphe 4.2.2.3.1) et 3, l'empreinte doit-elle être conservée au niveau du journal malgré un support WORM ?
	Réponse	1/ Oui, l'intégrité est assurée au plan technique dès le niveau 0, c'est-à-dire que les objets ne peuvent pas être modifiés ou supprimés. En revanche, la démontrabilité de cette intégrité n'intervient qu'à partir du niveau 2. 2/ Oui, l'empreinte doit être conservée au niveau du journal car elle contribue à la capacité à démontrer l'intégrité de l'archive
9	Question	Paragraphe 4.2.2.3.1 (niveau 2) : il est admis que le document à archiver puisse ne pas avoir d'empreinte associée et on la calcule alors. Pourtant, dans le paragraphe 5.1.2.3 décrivant le contrôle sur l'événement d'écriture d'archive pour le niveau 2, on compare par échantillonnage l'empreinte reçue avec l'empreinte de l'objet archivé. Au niveau 2, les documents reçus doivent-ils ou pas être accompagnés systématiquement de leur empreinte ?
	Réponse	Il n'est pas obligatoire que les documents reçus soient accompagnés systématiquement de leur empreinte. D'ailleurs, le contrôle de l'empreinte n'a lieu, par échantillonnage, que si l'archive réceptionnée est accompagnée de son empreinte.
10	Question	Paragraphe 4.2.2.4 : Quels éléments permettant de vérifier les signatures électroniques doivent être archivés dans un système tiers ?
	Réponse	Cela dépend du mécanisme de signature utilisé. Par exemple, pour des signatures asymétriques à clé publique, il faut le document original, le certificat du signataire, la chaine de confiance de l'AC émettrice du certificat, les CRL associées en vigueur au moment de la signature ou le jeton OCSP.
11	Question	Paragraphe 4.3.1 : description du journal des événements. *Ce journal se décompose en trois parties :* • *une partie pour les évènements relatifs à l'application d'archivage ;* • *une partie pour les évènements relatifs à la sécurité ;* • *une partie pour les évènements relatifs au système ;* 1 Pour chaque typologie d'événement, y a-t-il une liste d'événements devant obligatoirement figurer dans le journal des événements ? Si oui, laquelle ? 2 Si non, pouvez-vous donner des exemples d'événements applicatifs, d'événements de sécurité applicative, d'événements de sécurité système et d'événements système consignés dans le journal des événements ?
	Réponse	1/ Non il n'y a pas de liste fournie dans la norme AFNOR NF Z 42-013 2/ Exemples : - Evènement de sécurité : Erreur d'authentification utilisateur ou administrateur

Id	Q/R	Texte
		- Evènement applicatif : Arrêt/relance du SAE
12	Question	Paragraphe 5.1 : Les contrôles sur événement. Quelle différence y a-t-il entre les événements « Dépôt d'un objet à archiver » et « Ecriture d'une archive » ? Je comprends bien qu'il y a 2 actions successives, mais du point de vue du SAE, n'y a-t-il pas sollicitation par un seul événement qui est le dépôt de l'objet à archiver ?
	Réponse	Dans le cas du dépôt d'une unique archive, les 2 événements peuvent effectivement être vu comme un seul événement. Dans le cas du dépôt d'un lot d'archives, il y a bien l'événement de dépôt puis tous les événements « écriture d'archive » pour chaque archive.
13	Question	Paragraphe 5.1.1.3 (définition du contrôle sur l'événement « dépôt d'un objet à archiver » au niveau 2), paragraphe 5.1.2.3 (définition du contrôle sur l'événement « écriture d'une archive » au niveau 2), paragraphe 5.1.3.3 (définition du contrôle sur l'événement « lecture d'une archive » au niveau 2). Il est noté qu'en cas d'utilisation de WORM cryptographique, le contrôle d'intégrité est systématique. Ce contrôle est-il alors pris en charge entièrement par le support de stockage, sans traitement spécifique côté SAE ? Y a-t-il un impact pour le SAE ?
	Réponse	Dans le cas d'utilisation de WORM cryptographique(2), la responsabilité de l'intégrité de l'archive est du ressort du SAE. C'est dans le cas d'utilisation de WORM physique que l'intégrité est assurée par le support. (2) cf. Support niveaux de service d'archivage - Chap. 2 Définition du *W*orm cryptographique = *« Il s'agit de supports réinscriptibles protégés par des moyens cryptographiques tels que l'objet soit infalsifiable : garantie d'intégrité »*
14	Question	Paragraphe 5.2 (les contrôles récurrents). En cas d'utilisation de supports de stockage de type WORM cryptographique, y a-t-il nécessité de prévoir des traitements spécifiques de contrôle de l'intégrité du stock par le SAE ?
	Réponse	Oui … au niveau 2 par échantillonnage, … et au niveau 3 de façon exhaustive. Comme indiqué page 24 du document *« La périodicité des contrôles assurant la couverture complète peut varier selon les applications, notamment, selon le volume des archives. Elle est fixée par l'Etablissement »*
15	Question	Paragraphe 6 (Horodatage). Il est écrit en nota bene : *L'objet archivé peut contenir des éléments de preuve intrinsèquement.* Pouvez-vous détailler ? Dans quels cas un objet archivé contient-il des éléments de preuve intrinsèquement ? Quel est l'impact pour le SAE ?
	Réponse	Au premier chef, le NB s'avère superfétatoire. Sa suppression sera proposée dans une prochaine version. Il avait pour objectif de prévenir le lecteur sur le fait que des archives pouvaient porter en elles-mêmes des preuves intrinsèques (ex : signature électronique, horodatage, scellement,…), autant d'éléments que le SAE aura dû contrôler au moment du dépôt en fonction du niveau de service retenu.

Id	Q/R	Texte
16	Question	(complément à la question 5) A quoi correspond un profil d'archivage ?
	Réponse	Voir réponse question 5
17	Question	Quand les archives arrivées au terme de leur durée de conservation sont détruites automatiquement par le SAE par application du sort final, y a-t-il aussi nécessité de vérifier la signature électronique de l'ordre de suppression ?
	Réponse	Lorsque la suppression est automatique, il n'y a pas d'ordre donné pour ce faire, donc pas de signature du donneur d'ordre à contrôler.
18	Question	Dans le niveau 3 du support CFONB, quels événements sur l'archive et quels traitements du SAE nécessitent un jeton d'horodatage ? Y a-t-il besoin d'un jeton d'horodatage seulement lors du dépôt de document, ou bien chaque événement journalisé nécessite-t-il un jeton d'horodatage ?
	Réponse	Au niveau 3, tous les événements sur l'archive ou traitements du SAE doivent être horodatés avec délivrance d'un jeton d'horodatage.