Mesures de sécurité de pseudonymisation des logiciels PMSI

A la demande de la Cnil, l'ATIH a intégré un mécanisme de chiffrement des fichiers PMSI contenant la correspondance entre les pseudonymes (issus du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR), et les identités (numéro administratif) des patients.
Ce mécanisme, généré sur les postes de travail, modifie les données accessibles aux établissements.

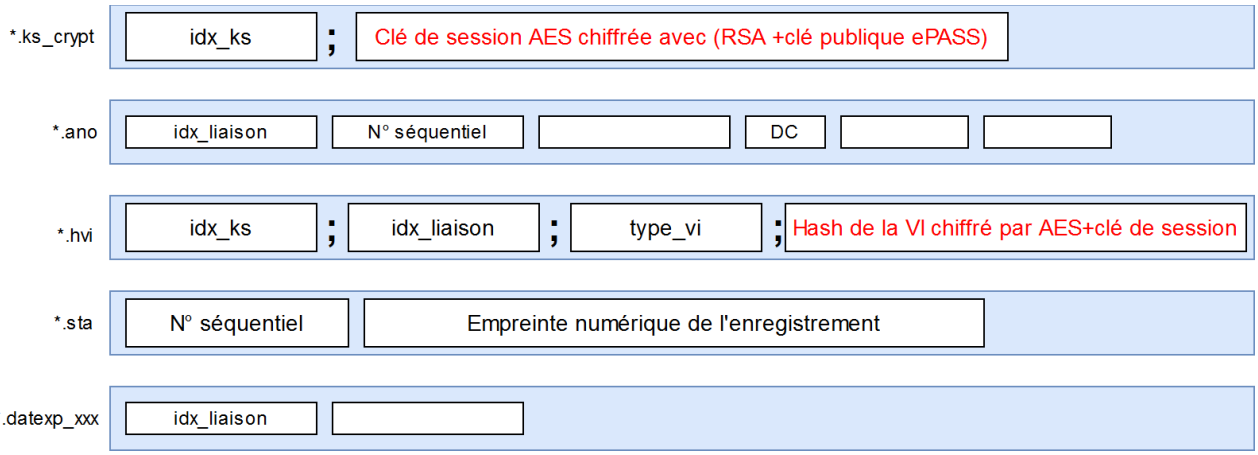
Les formats d'entrée des logiciels déjà mis à disposition ne seront pas modifiés. Le NIR ainsi que les autres variables identifiantes dans les recueils (IPP ou le numéro administratif de la mère) ont fait l'objet d'opération de pseudonymisation et de chiffrement.

Les pseudonymes n'apparaissent plus dans les fichiers ANO. Ils sont désormais hachés, chiffrés et stockés dans un fichier spécifique. Le lien entre ce fichier spécifique et le fichier ANO est assuré par l'ajout d'une variable de liaison en début des fichiers ANO (32 caractères). Cette variable de liaison est non signifiante.
L'algorithme de chiffrement produit un résultat différent à chaque appel. Autrement dit un même pseudonyme aura à chaque opération de chiffrement une valeur différente, ce qui empêche l'élaboration d'une table de correspondance.

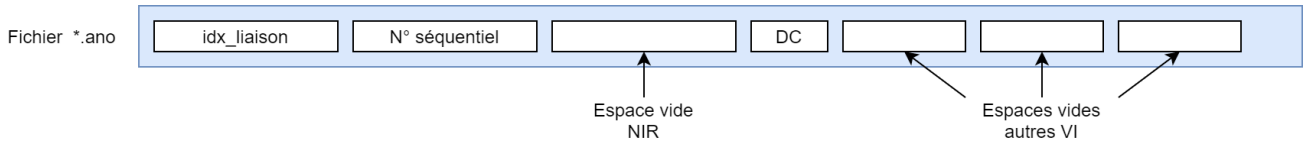
Dans les établissements ex-DG à partir de M3, pour l'activité d'hospitalisation, en sortie de MAGIC, le fichier ANOHOSP contient le NIR pseudonymisé chiffré en fin d'enregistrement. Lors du traitement par GENRSA, le NIR pseudonymisé chiffré va se retrouver dans un nouveau fichier en sortie (*.hnir) en M3 ou dans fichier (*.hvi) à partir de M4. Comme indiqué plus haut, GENRSA va également traiter les autres variables identifiantes du fichier ANOHOSP de la même façon. Celles-ci seront hachées, chiffrées et intégrées dans les fichiers (*.hvi).
Dans les établissements ex-OQN, ou pour l'activité externe des ex-DG, toutes les opérations de chiffrement seront réalisées par les logiciels AGRAF ou PREFACE. On obtiendra donc en sortie des fichiers (*.hnir) en M3 et des fichiers (*.hvi) suivant les mêmes procédures que pour les établissements ex-DG.
Dans les deux cas, le fichier ANO sera modifié par l'intégration de la variable de liaison en début d'enregistrement (32 caractères).

Afin d'améliorer les temps de traitement tout en conservant un haut niveau de sécurité, l'algorithme de chiffrement du NIR pseudonymisé a été ajusté, entre les transmissions M3 et M4. L'algorithme utilisé en M3 était un RSA-2048 avec la clé publique de e-PASS.
À partir des transmissions de M4, l'algorithme de chiffrement des variables identifiantes est AES-256, associé à une clé de session générée par chaque logiciel (MAGIC et GENRSA). Ces clés sont différentes à chaque lancement des logiciels. Les clés de sessions seront-elles-même chiffrées par l'algorithme RSA-2048 avec la clé publique de e-PASS, et intégrée dans le fichier (*.ks_crypt).

Ces schémas représentent de manière simplifiée les formats des différents fichiers.



Focus sur fichier *.ano



L'idx_ks correspond à un identifiant de clé pour gérer le cas où on a plusieurs clés de session. Par exemple dans les exDG, à partir de M4, on aura au minimum 2 clés de sessions : une pour MAGIC et une pour GENRSA.

Tableau ci-dessous liste les VI (Variables Identifiantes) avec le code type_vi tel qu'attendu par e-PMSI dans le fichier *.hvi.

	Nom	**Code e-PMSI**
1	NIR pseudonymisé	tvi_hnir
2	IPP	tvi_ipp
3	N° admin de la mère	tvi_nadmin
4	Empreinte Lamda	tvi_emplamda
5	N° facture mère	tvi_nfactmere
6	IPP externe (pour la psychiatrie)	tvi_ipp_ext