

Programme Identifiant National de Santé

Algorithme de calcul de l'INS-C

Juin 2009

Sommaire

1	Objet.....	3
2	Spécifications de l'INS-C.....	3
2.1	Principe général de calcul de l'INS-C.....	3
2.2	Format de l'INS-C.....	3
2.3	Normalisation des données.....	4
2.3.1	Caractères acceptés en entrée de la fonction de calcul de l'INS-C.....	4
2.3.2	Normalisation des caractères.....	4
2.3.3	Traitement des champs vides.....	6
2.4	Algorithme de calcul de l'INS-C.....	6
2.4.1	Données en entrée.....	6
2.4.2	Contrôle avant calcul.....	7
2.4.3	Normalisation des champs avant calcul.....	7
2.4.4	Calcul de l'INS-C.....	7
3	Annexe 1 : Exemples de codes de calcul de l'INS-C.....	8

1 Objet

Ce document est le document de spécifications de l'algorithme pour le calcul de l'INS-C.

2 Spécifications de l'INS-C

2.1 Principe général de calcul de l'INS-C

L'INS-C est obtenu en appliquant un algorithme défini par le ministère de la santé avec le concours de la DCSSI à un nombre limité de traits d'identité de la personne concernée.

Les traits d'identité retenus sont les suivants :

- Le NIR de la personne concernée
- Les prénoms de la personne concernée
- La date de naissance de la personne concernée

L'algorithme de calcul est spécifié plus loin dans le présent document.

Les données sont lues dans la puce de la carte Vitale présentée par le patient.

Il s'agit des traits d'identité de la personne concernée (bénéficiaire ayant droit ou ouvrant droit) et non de son ouvrant droit si la personne concernée est un ayant-droit.

Il est obligatoire d'utiliser les traits lus dans la carte Vitale.

2.2 Format de l'INS-C

L'INS-C est composé de 20 caractères numériques auquel s'ajoute une clé de contrôle de 2 chiffres.

Il est complété par un préfixe de 3 caractères représentant un code national (code ISO de la France : 250).

Le préfixe signifie que l'identifiant a été attribué par le système de gestion des INS-C français. L'usage du préfixe est implicite au sein des systèmes de santé français (s'il est absent, les systèmes de santé le complètent automatiquement).

Exemple : 250 15489609345890393434 76

250 15489609345890393434 76

Préfixe ISO | INS calculé | clé de contrôle

Le préfixe ISO n'est pas pris en compte dans le calcul de la clé de contrôle

La clé de contrôle est calculée selon la même règle que la clé du NIR : la clé est égale au complément à 97 du reste de la division euclidienne de l'INS calculé par 97.

2.3 Normalisation des données

Les traits d'identité doivent, si nécessaire, faire l'objet d'une normalisation avant le calcul.

2.3.1 Caractères acceptés en entrée de la fonction de calcul de l'INS-C

L'algorithme de calcul de l'INS-C n'accepte en entrée que les caractères alphanumériques encodés au format ASCII définis dans le tableau suivant. Pour information, cette définition est celle sur type de données « CA : Caractères alphanumériques » défini dans le manuel de programmation des services SESAM-Vitale 1.40.x

Type de données	Caractères	Encodage ASCII correspondant
CA	Chiffres de '0' à '9'	'0' (0x30) à '9' (0x39)
	Lettres alphabétiques majuscules non accentuées ('A' à 'Z')	'A' (0x41) à 'Z' (0x5A)
	Espace	' ' (0x20)

2.3.2 Normalisation des caractères

Quel que soit l'encodage d'origine des données (ISO-8859-1, EBCDIC...), les caractères constitutifs des données doivent être normalisés selon les règles décrites dans les tableaux suivants.

Caractère d'origine quelque soit l'encodage. Les caractères présentés dans le présent tableau sont ceux retenus par le standard ISO 8859-1	Valeur normalisée de remplacement du caractère.	Encodage ASCII du
Caractères alphabétiques minuscules non accentués ('a' à 'z')	Caractère alphabétique majuscule correspondant non accentué	'A' (0x41) à 'Z' (0x5A)

Caractère d'origine quelque soit l'encodage. Les caractères présentés dans le présent tableau sont ceux retenus par le standard ISO 8859-1	Valeur normalisée de remplacement caractère.	de du	Encodage ASCII
Caractères majuscules non accentués ('A' à 'Z')	Caractère alphabétique majuscule correspondant non accentué		'A' (0x41) à 'Z' (0x5A)
Caractère accentués : À Á Â Ã Ä Å Æ à á â ã æ ä å	A majuscule		'A' (0x41)
Caractère accentués : È É Ê Ë è é ê ë	E majuscule		'E' (0x45)
Caractère accentués : Đ đ	D majuscule		'D' (0x44)
Caractère accentués : Ò Ó Ô Õ Ö Ø ò ó ô õ ö ø	O majuscule		'O' (0x4F)
Caractère accentués : Ý ý ÿ	Y majuscule		'Y' (0x59)
Caractère accentués : Ç ç	C majuscule		'C' (0x43)
Caractère accentués : ì í î ï ï ï	I majuscule		'I' (0x49)
Caractère accentués : Ñ ñ	N majuscule		'N' (0x4E)
Caractère accentués : Ù Ú Û Ü ú û ü	U majuscule		'U' (0x55)
Caractère accentués : ß	B majuscule		'B' (0x42)
Tous les autres caractères (! « # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ' { } ~ NBSP ¡ ¢ £ ¤ ¥ ¦ § ¨ (c) ª « ¬ - (r) ° ± ² ³ ´ µ ¶ · ¸ ¹ º « ¼ ½ ¾ ¿ × ÷ ð	Caractère Espace		' ' (0x20)

Cas des caractères non pris en charge par la norme ISO8859-1 :

Caractère d'origine quelque soit l'encodage.	Valeur normalisée de remplacement	Encodage ASCII
Œ et œ	OE	'OE' (0x4F, 0x45)
Š š	S	'S' (0x53)
Ž ž	Z	'Z' (0x5A)
ÿ	Y	'Y' (0x59)
Tout autre caractère	Caractère Espace	' ' (0x20)

Remarque sur le format des données

L'objectif de la normalisation des données est d'avoir une représentation identique des données quelque soit l'origine des données. Ainsi, le choix s'est porté vers une simplification des caractères afin d'avoir un minimum d'impact sur les logiciels de PS et de ne pas imposer le support de jeux de caractères plus complexes que l'ASCII.

2.3.3 Traitement des champs vides

Si le champ prénom est vide, il doit être renseigné au moins par un caractère espace en entrée de la fonction de calcul de l'INS-C.

Si le champ date de naissance est vide, il doit être renseigné à la valeur 000000 en entrée de la fonction de calcul de l'INS-C.

2.4 Algorithme de calcul de l'INS-C

2.4.1 Données en entrée

Il s'agit des données dont les caractères ont été normalisés selon les règles exposées au chapitre précédent.

Données	Format	Description
NIR	CA	NIR de la personne sur 13 caractères Il s'agit du NIR du bénéficiaire lu dans la carte Vitale dans le champ « NIR certifié », ou du NIR lu dans le champ « NIR » si le champ « NIR certifié » n'est pas renseigné.
Clé du NIR	CA	Clé du NIR sur 2 caractères
Prénoms	CA	Prénoms du patient.
Date de naissance	CA	Date de naissance au format AAMMJJ

2.4.2 Contrôle avant calcul

Un contrôle de cohérence entre le NIR et la clé du NIR doit être fait avant le calcul de l'INS-C. En cas d'incohérence entre le NIR et la clé du NIR, le calcul de l'INS-C est abandonné.

Le calcul est également abandonné si le NIR correspond à un NIR temporaire.

2.4.3 Normalisation des champs avant calcul

NIR

Les 13 caractères alphanumériques du NIR sont utilisés. La clé du NIR est utilisée pour contrôler la valeur du NIR.

Prénoms

Si le patient a plusieurs prénoms, les prénoms sont susceptibles d'être séparés par un ou plusieurs espaces.

Il s'agit dans une première étape de supprimer tous les espaces, puis de retenir les 10 premiers caractères de la chaîne ainsi obtenue. Si la chaîne résultante est constituée de moins de 10 caractères, elle est complétée à droite par des espaces (0x20).

Date de naissance

Le format AAMMJJ sur 6 caractères numériques est utilisé

2.4.4 Calcul de l'INS-C

1. Récupérer les données nécessaires au calcul (lecture de la carte Vitale) : NIR, prénoms et date de naissance de la personne concernée.
2. Normaliser les données selon les règles énoncées plus haut dans l'ordre suivant :
 - a. normalisation des caractères
 - b. puis normalisation des champs.

3. Concaténer sans séparateur les trois champs dans l'ordre suivant : Prénoms, date de naissance puis NIR.

L'ensemble concaténé constitue la « graine ».

Graine = Prénoms (10 caractères) + Date de naissance (6 caractères) + NIR (13 caractères).

4. Calculer le haché de la chaîne de caractères 'Graine' au moyen de la fonction SHA256 (cf. le référentiel cryptographique de la DCSSI)

Le résultat obtenu est une empreinte de 256 bits.

5. Conversion de l'empreinte en format numérique (chiffres de 0 à 9)

Les 64 bits de poids fort de l'empreinte sont convertis en base 10 afin d'obtenir une chaîne composée de 20 chiffres. Si le nombre obtenu s'exprime sur moins de 20 chiffres, il est complété à gauche par des zéros.

6. Calcul de l'INS-C

L'INS-C est constitué du nombre de 20 chiffres obtenu à l'étape précédente complété par une clé de contrôle sur 2 chiffres.

La clé de contrôle est calculée selon la même règle que la clé du NIR : la clé est égale au complément à 97 du reste de la division euclidienne du nombre de 20 chiffres par 97.

3 Annexe 1 : Exemples de codes de calcul de l'INS-C

Rédaction réservée.