DÉCISION 2008/616/JAI DU CONSEIL

du 23 juin 2008

concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière

LE CONSEIL DE L'UNION EUROPÉENNE,

vu l'article 33 de la décision 2008/615/JAI du Conseil [1],

vu l'initiative de la République fédérale d'Allemagne,

vu l'avis du Parlement européen [2],

considérant ce qui suit:

(1) Le 23 juin 2008, le Conseil a adopté la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

(2) Par la décision 2008/615/JAI, les éléments fondamentaux du traité du 27 mai 2005 entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale (ci-après dénommé «traité de Prüm») ont été transposés dans le cadre juridique de l'Union européenne.

(3) L'article 33 de la décision 2008/615/JAI dispose que le Conseil doit arrêter les mesures nécessaires pour mettre en œuvre la décision 2008/615/JAI au niveau de l'Union, conformément à la procédure prévue à l'article 34, paragraphe 2, point c), deuxième phrase, du traité sur l'Union européenne. Il y a lieu que ces mesures se fondent sur l'accord d'exécution du 5 décembre 2006 concernant la mise en œuvre administrative et technique et l'exécution du traité de Prüm.

(4) La présente décision établit les dispositions normatives communes qui sont indispensables à la mise en œuvre administrative et technique des formes de coopération prévues dans la décision 2008/615/JAI. L'annexe de la présente décision contient les dispositions d'exécution à caractère technique. En outre, un manuel distinct, comprenant exclusivement les informations factuelles que les États membres fourniront, sera élaboré et tenu à jour par le secrétariat général du Conseil.

(5) Compte tenu des capacités techniques, la recherche de nouveaux profils ADN à caractère routinier sera en principe effectuée au moyen de consultations spécifiques, et il conviendra de trouver au niveau technique les solutions adéquates à cette fin,

DÉCIDE:

CHAPITRE I

GÉNÉRALITÉS

Article premier

Objet

La présente décision a pour objet d'établir les dispositions administratives et techniques nécessaires à la mise en œuvre de la décision 2008/615/JAI, en particulier en ce qui concerne les échanges automatisés des données ADN, des données dactyloscopiques et des données relatives à l'immatriculation des véhicules prévus au chapitre 2 de la présente décision, ainsi que pour les autres formes de coopération visées au chapitre 5 de la présente décision.

Article 2

Définitions

Aux fins de la présente décision, on entend par:

a) «consultation» et «comparaison» telles que visées aux articles 3, 4 et 9 de la décision 2008/615/JAI, les procédures par lesquelles il est établi qu'il y a une concordance entre, respectivement, des données ADN ou des données dactyloscopiques communiquées par un État membre et des données ADN ou des données dactyloscopiques contenues dans les bases de données d'un, de plusieurs, ou de tous les États membres;

b) «consultation automatisée» telle que visée à l'article 12 de la décision 2008/615/JAI, l'accès en ligne permettant de consulter les bases de données d'un, de plusieurs, ou de tous les États membres;

c) «profil ADN», un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci);

d) «partie non codante de l'ADN», les régions chromosomiques non génétiquement exprimées, c'est-à-dire non connues pour fournir des propriétés fonctionnelles d'un organisme;

[1] Voir page 1 du présent Journal officiel.
[2] Avis du 21 avril 2008 (non encore paru au Journal officiel).

e) «données indexées ADN», un profil ADN et une référence;

f) «profil ADN de référence», le profil ADN d'une personne identifiée;

g) «profil ADN non identifié», le profil ADN obtenu à partir de traces recueillies lors d'une enquête pénale et appartenant à une personne non encore identifiée;

h) «annotation», une marque insérée par un État membre sur un profil ADN contenu dans sa base de données nationale afin d'indiquer que ce profil ADN a déjà fait l'objet d'une concordance lors d'une consultation ou d'une comparaison effectuée par un autre État membre;

i) «données dactyloscopiques», les images d'empreintes digitales, images d'empreintes digitales latentes, d'empreintes de paumes de mains, d'empreintes de paumes de mains latentes, ainsi que des modèles de telles images (points caractéristiques codés), lorsqu'ils sont stockés et traités dans une base de données automatisée;

j) «données relatives à l'immatriculation des véhicules», l'ensemble des données visé au chapitre 3 de l'annexe;

k) «cas par cas», par référence à l'article 3, paragraphe 1, deuxième phrase, à l'article 9, paragraphe 1, deuxième phrase, et à l'article 12, paragraphe 1, de la décision 2008/615/JAI, une seule enquête ou un seul dossier de poursuites pénales. Si ce dossier concerne plus d'un profil ADN, d'une donnée dactyloscopique ou d'une donnée relative à l'immatriculation des véhicules, ces profils ou ces données peuvent être transmis ensemble en une seule demande.

CHAPITRE 2

DISPOSITIONS COMMUNES EN MATIÈRE D'ÉCHANGE DE DONNÉES

Article 3

Spécifications techniques

Les États membres observent les spécifications techniques communes dans le cadre de toutes les demandes et réponses liées aux consultations et comparaisons de profils ADN, de données dactyloscopiques et de données relatives à l'immatriculation des véhicules. Ces spécifications techniques sont définies à l'annexe de la présente décision.

Article 4

Réseau de communication

L'échange électronique de données ADN, de données dactyloscopiques et de données relatives à l'immatriculation des véhicules entre les États membres s'effectue via le réseau de communication «Services télématiques transeuropéens sécurisés entre administrations (TESTA II)» et ses nouvelles versions.

Article 5

Disponibilité des échanges de données automatisés

Les États membres prennent toutes les mesures nécessaires pour que la consultation ou la comparaison automatisée de données ADN, de données dactyloscopiques et de données relatives à l'immatriculation de véhicules soit possible 24 heures sur 24 et 7 jours sur 7. Dans l'éventualité d'une défaillance technique, les points de contact nationaux des États membres s'en informent immédiatement et conviennent d'un autre système d'échange d'informations à titre temporaire, conformément aux dispositions juridiques applicables. L'échange automatisé des données est remis en service aussi rapidement que possible.

Article 6

Références des données ADN et des données dactyloscopiques

Les références visées à l'article 2 et à l'article 8 de la décision 2008/615/JAI consistent en la combinaison des éléments suivants:

a) un code permettant aux États membres, en cas de concordance, d'extraire des données à caractère personnel et d'autres informations de leur base de données afin de les transmettre à un, à plusieurs ou à tous les États membres, conformément à l'article 5 ou à l'article 10 de la décision 2008/615/JAI;

b) un code pour indiquer l'origine nationale du profil ADN ou des données dactyloscopiques; et

c) pour les données ADN, un code pour indiquer le type de profil ADN.

CHAPITRE 3

DONNÉES ADN

Article 7

Principes régissant l'échange de données ADN

1. Les États membres utilisent les normes existantes en matière d'échange de données ADN, telles que l'ensemble européen de référence (European Standard Set, ESS) ou le groupe standard de loci d'Interpol (Interpol Standard Set of Loci, ISSOL).

2. La procédure de transmission, en cas de consultation et de comparaison automatisées de profils ADN, s'effectue dans le cadre d'une structure décentralisée.

3. Des mesures appropriées sont prises pour assurer la confidentialité et l'intégrité des données transmises aux autres États membres, notamment en matière de cryptage.

4. Les États membres prennent les mesures nécessaires pour garantir l'intégrité des profils ADN mis à la disposition des autres États membres ou transmis pour comparaison et pour faire en sorte que ces mesures soient conformes aux normes internationales, telles que l'ISO 17025.

5. Les États membres utilisent les codes «États membres» selon la norme ISO 3166-1 alpha-2.

Article 8

Règles applicables aux demandes et réponses relatives aux données ADN

1. Une demande de consultation ou de comparaison automatisée telle que visée à l'article 3 ou à l'article 4 de la décision 2008/615/JAI inclut uniquement les informations suivantes:

a) le code «État membre» de l'État membre requérant;

b) la date, l'heure et le numéro de référence de la demande;

c) les profils ADN et leurs références;

d) les types de profils ADN transmis (profils ADN non identifiés ou profils ADN de référence); et

e) les informations requises pour contrôler les systèmes de bases de données et pour le contrôle de la qualité des procédures de consultation automatisée.

2. La réponse (rapport de concordance) apportée à la demande visée au paragraphe 1 inclut uniquement les informations suivantes:

a) une indication précisant s'il y a eu une ou plusieurs concordances («hit») ou aucune concordance («no hit»);

b) la date, l'heure et le numéro de référence de la demande;

c) la date, l'heure et le numéro de référence de la réponse;

d) le code «État membre» de l'État membre requérant et de l'État membre requis;

e) le numéro de référence de l'État membre requérant et de l'État membre requis;

f) le type de profils ADN transmis (profil ADN non identifié ou profil ADN de référence);

g) les profils ADN demandés et ceux pour lesquels une concordance est établie; et

h) les informations requises pour contrôler les systèmes de bases de données et pour le contrôle de la qualité des procédures de consultation automatisée.

3. La notification automatisée d'une concordance est effectuée uniquement si la consultation ou la comparaison automatisée a mis en évidence une concordance fondée sur un nombre minimal de loci. Ce minimum est fixé au chapitre 1 de l'annexe de la présente décision.

4. Les États membres prennent les mesures nécessaires pour que les demandes soient conformes aux déclarations communiquées en vertu de l'article 2, paragraphe 3, de la décision 2008/615/JAI. Ces déclarations figurent dans le manuel visé à l'article 18, paragraphe 2, de la présente décision.

Article 9

Procédure de transmission applicable à la consultation automatisée de profils ADN non identifiés conformément à l'article 3 de la décision 2008/615/JAI

1. Si, en cas de consultation à partir d'un profil ADN non identifié, la base de données nationale n'a mis en évidence aucune concordance ou a mis en évidence une concordance avec un profil ADN non identifié, ce profil ADN non identifié peut être transmis aux bases de données de tous les autres États membres et si, en cas de consultation à partir du profil ADN susvisé, les bases de données des autres États membres mettent en évidence des concordances avec des profils ADN de référence et/ou des profils ADN non identifiés, ces concordances sont automatiquement communiquées et les données indexées ADN sont transmises à l'État membre requérant; si les bases de données des autres États membres ne mettent en évidence aucune concordance, l'État membre requérant en est automatiquement informé.

2. Si, en cas de consultation à partir d'un profil ADN non identifié, les bases de données des autres États membres mettent en évidence une concordance, chaque État membre concerné peut insérer une annotation dans ce sens dans sa base de données nationale.

Article 10

Procédure de transmission applicable à la consultation automatisée de profils ADN de référence conformément à l'article 3 de la décision 2008/615/JAI

Si, en cas de consultation à partir d'un profil ADN de référence, la base de données nationale n'a mis en évidence aucune concordance avec un profil ADN de référence ou a mis en évidence une concordance avec un profil ADN non identifié, le profil ADN de référence concerné peut être transmis aux bases de données de tous les autres États membres, et si, en cas de consultation à partir du profil ADN de référence susvisé, les bases de données des autres États membres mettent en évidence des concordances avec des profils ADN de référence et/ou des profils ADN non identifiés, ces concordances sont automatiquement communiquées et les données indexées ADN sont transmises à l'État membre requérant; si les bases de données des autres États membres ne mettent en évidence aucune concordance, l'État membre requérant en est automatiquement informé.

Article 11

Procédure de transmission applicable à la comparaison automatisée de profils ADN non identifiés conformément à l'article 4 de la décision 2008/615/JAI

1. Si, en cas de comparaison avec des profils ADN non identifiés, les bases de données des autres États membres mettent en évidence des concordances avec des profils ADN de référence et/ou des profils ADN non identifiés, ces concordances sont automatiquement communiquées et les données indexées ADN sont transmises à l'État membre requérant.

2. Si, en cas de comparaison avec des profils ADN non identifiés, les bases de données des autres États membres mettent en évidence des concordances avec des profils ADN non identifiés ou des profils ADN de référence, chaque État membre concerné peut insérer une annotation dans ce sens dans sa base de données nationale.

CHAPITRE 4

DONNÉES DACTYLOSCOPIQUES

Article 12

Principes régissant l'échange de données dactyloscopiques

1. La numérisation des données dactyloscopiques et leur transmission aux autres États membres s'effectuent selon un format de données uniforme, décrit au chapitre 2 de l'annexe.

2. Chaque État membre s'assure que les données dactyloscopiques qu'il transmet sont d'une qualité suffisante en vue d'une comparaison par les fichiers automatisés d'empreintes digitales (FAED).

3. La procédure de transmission applicable à l'échange de données dactyloscopiques est mise en œuvre dans le cadre d'une structure décentralisée.

4. Des mesures appropriées sont prises pour assurer la confidentialité et l'intégrité des données dactyloscopiques transmises aux autres États membres, notamment en matière de cryptage.

5. Les États membres utilisent les codes «États membres» selon la norme ISO 3166-1 alpha-2.

Article 13

Capacités de consultation pour les données dactyloscopiques

1. Chaque État membre veille à ce que ses demandes de consultation ne dépassent pas les capacités de consultation indiquées par l'État membre requis. Les États membres adressent au secrétariat général du Conseil les déclarations visées à l'article 18, paragraphe 2, indiquant leurs capacités maximales de consultation journalières pour les données dactyloscopiques de personnes identifiées ou pour les données dactyloscopiques de personnes non encore identifiées.

2. Le nombre maximal de candidats admis par transmission pour vérification est fixé au chapitre 2 de l'annexe.

Article 14

Règles applicables aux demandes et aux réponses relatives aux données dactyloscopiques

1. L'État membre requis contrôle sans tarder, par un procédé entièrement automatisé, la qualité des données dactyloscopiques transmises. Au cas où les données ne se prêtent pas à une comparaison automatisée, l'État membre requis en informe sans tarder l'État membre requérant.

2. L'État membre requis effectue les consultations dans l'ordre chronologique d'arrivée des demandes. Les demandes doivent être traitées dans les vingt-quatre heures par un procédé entièrement automatisé. L'État membre requérant peut, si sa législation nationale l'exige, demander le traitement accéléré de ses demandes et l'État membre requis effectue la consultation sans tarder. Si les délais ne peuvent pas être respectés pour des raisons de force majeure, la comparaison est effectuée sans tarder dès que les obstacles ont été levés.

CHAPITRE 5

DONNÉES RELATIVES À L'IMMATRICULATION DES VÉHICULES

Article 15

Principes régissant la consultation automatisée de données relatives à l'immatriculation des véhicules

1. Pour la consultation automatisée de données relatives à l'immatriculation des véhicules, les États membres utilisent une version de l'application informatique du système d'information européen concernant les véhicules et les permis de conduire (Eucaris) spécialement conçue aux fins de l'article 12 de la décision 2008/615/JAI, ainsi que les versions modifiées de cette application.

2. La consultation automatisée de données relatives à l'immatriculation des véhicules s'effectue dans le cadre d'une structure décentralisée.

3. Les informations échangées via le système Eucaris sont transmises sous une forme cryptée.

4. Les éléments de données relatives à l'immatriculation des véhicules qui doivent être échangées sont décrits au chapitre 3 de l'annexe.

5. Dans le cadre de la mise en œuvre de l'article 12 de la décision 2008/615/JAI, les États membres peuvent donner la priorité aux consultations liées à la lutte contre la grande criminalité.

Article 16

Coûts

Chaque État membre prend en charge les coûts afférents à la gestion, à l'utilisation et à la maintenance de l'application informatique Eucaris visée à l'article 15, paragraphe 1.

CHAPITRE 6

COOPÉRATION POLICIÈRE

Article 17

Patrouilles communes et autres opérations conjointes

1. Conformément au chapitre 5 de la décision 2008/615/JAI, et en particulier aux déclarations communiquées au titre de l'article 17, paragraphe 4, et de l'article 19, paragraphes 2 et 4, de la présente décision, chaque État membre désigne un ou plusieurs

points de contact afin de permettre aux autres États membres de s'adresser aux autorités compétentes, et chaque État membre peut préciser ses procédures pour l'organisation de patrouilles communes ou d'autres opérations conjointes, ses procédures à l'égard des initiatives des autres États membres concernant ces opérations, ainsi que d'autres aspects pratiques, et les modalités opérationnelles applicables à ces opérations.

2. Le secrétariat général du Conseil établit et tient à jour une liste des points de contact et informe les autorités compétentes de toute modification de cette liste.

3. Les autorités compétentes de chaque État membre peuvent prendre une initiative visant à mettre en place une opération conjointe. Avant le commencement d'une opération donnée, les autorités compétentes visées au paragraphe 2, déterminent, verbalement ou par écrit, les dispositions relatives aux modalités telles que:

a) les autorités des États membres compétentes pour l'opération;

b) le but précis de l'opération;

c) l'État membre d'accueil où l'opération doit avoir lieu;

d) la zone géographique de l'État membre d'accueil où l'opération doit avoir lieu;

e) la période couverte par l'opération;

f) l'assistance spécifique à fournir par le ou les États membres d'origine à l'État membre d'accueil, y compris des fonctionnaires ou d'autres agents de l'autorité publique, des éléments matériels ou financiers;

g) les fonctionnaires participant à l'opération;

h) le fonctionnaire responsable de l'opération;

i) les attributions que les fonctionnaires et autres agents de l'autorité publique du ou des États membres d'origine peuvent exercer dans l'État membre d'accueil pendant l'opération;

j) les armes, munitions et équipements particuliers que les fonctionnaires de l'État membre d'origine peuvent utiliser pendant l'opération conformément à la décision 2008/615/JAI;

k) les modalités logistiques relatives au transport, à l'hébergement et à la sécurité;

l) la répartition des coûts de l'opération conjointe, si elle diffère des dispositions prévues à l'article 34, première phrase, de la décision 2008/615/JAI;

m) tout autre élément nécessaire, le cas échéant.

4. Les déclarations, procédures et désignations prévues au présent article figurent dans le manuel visé à l'article 18, paragraphe 2.

CHAPITRE 7

DISPOSITIONS FINALES

Article 18

Annexe et manuel

1. L'annexe de la présente décision fixe les autres modalités applicables à la mise en œuvre technique et administrative de la décision 2008/615/JAI.

2. Un manuel est élaboré et tenu à jour par le secrétariat général du Conseil; il comprend exclusivement les informations factuelles fournies par les États membres, par le biais de déclarations faites conformément à la décision 2008/615/JAI ou à la présente décision ou de notifications faites au secrétariat général du Conseil. Ce manuel se présente sous la forme d'un document du Conseil.

Article 19

Autorités indépendantes compétentes en matière de protection des données

Conformément à l'article 18, paragraphe 2, les États membres communiquent au secrétariat général du Conseil le nom des autorités indépendantes compétentes en matière de protection des données ou des autorités judiciaires visées à l'article 30, paragraphe 5, de la décision 2008/615/JAI.

Article 20

Élaboration des décisions visées à l'article 25, paragraphe 2, de la décision 2008/615/JAI

1. Le Conseil prend la décision visée à l'article 25, paragraphe 2, de la décision 2008/615/JAI sur la base d'un rapport d'évaluation fondé sur un questionnaire.

2. En ce qui concerne l'échange automatisé de données visé au chapitre 2 de la décision 2008/615/JAI, le rapport d'évaluation est aussi fondé sur une visite d'évaluation et un essai pilote effectué lorsque l'État membre concerné a communiqué au secrétariat général du Conseil les informations visées à l'article 36, paragraphe 2, première phrase, de la décision 2008/615/JAI.

3. D'autres modalités pour cette procédure sont exposées au chapitre 4 de l'annexe.

Article 21

Évaluation de l'échange d'informations

1. L'application, d'un point de vue administratif, technique et financier, de l'échange d'informations au titre du chapitre 2 de la décision 2008/615/JAI, et notamment le recours au mécanisme prévu à l'article 15, paragraphe 5, fait l'objet d'une évaluation à intervalles réguliers. L'évaluation concerne les États membres qui appliquent déjà la décision 2008/615/JAI au moment de l'évaluation et porte sur les catégories de données pour lesquelles

l'échange d'informations a commencé entre les États membres concernés. L'évaluation est fondée sur des rapports présentés par chacun de ces États membres.

2. D'autres modalités pour cette procédure sont exposées au chapitre 4 de l'annexe.

Article 22

Rapport avec l'accord d'exécution du traité de Prüm

Pour les États membres qui sont liés par le traité de Prüm, les dispositions concernées de la présente décision et de son annexe, lorsqu'elles seront pleinement en vigueur, s'appliquent en lieu et place des dispositions correspondantes contenues dans l'accord d'exécution du traité de Prüm. Toutes les autres dispositions de l'accord d'exécution restent applicables entre les parties contractantes au traité de Prüm.

Article 23

Mise en œuvre

Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision dans les délais prévus à l'article 36, paragraphe 1, de la décision 2008/615/JAI.

Article 24

Application

La présente décision prend effet vingt jours après sa publication au *Journal officiel de l'Union européenne*.

Fait à Luxembourg, le 23 juin 2008.

Par le Conseil

Le président

I. JARC

ANNEXE

TABLE DES MATIÈRES

CHAPITRE 1: **Échange de données ADN**

1. ***Questions de criminalistique et règles et algorithmes de concordance dans le domaine génétique***

1.1. *Propriétés des profils ADN*

1.2. *Règles de concordance*

1.3. *Règles en matière de rapports*

2. ***Tableau des codes des États membres***

3. ***Analyse fonctionnelle***

3.1. *Disponibilité du système*

3.2. *Deuxième étape*

4. ***Document de contrôle des interfaces ADN***

4.1. *Introduction*

4.2. *Définition de la structure XML*

5. ***Application, sécurité et architecture de communication***

5.1. *Présentation*

5.2. *Architecture de haut niveau*

5.3. *Normes de sécurité et protection des données*

5.4. *Protocoles et normes à mettre en œuvre pour le cryptage: S/MIME et mécanismes connexes*

5.5. *Architecture de l'application*

5.6. *Protocoles et normes à utiliser dans l'architecture de l'application*

5.7. *Cadre de communication*

CHAPITRE 2: **Échange de données dactyloscopiques (document de contrôle des interfaces)**

1. ***Aperçu de la teneur des fichiers***

2. ***Format des enregistrements***

3. ***Enregistrement logique de type 1: en-tête de fichier***

4. ***Enregistrement logique de type 2: descriptif***

5. ***Enregistrement logique de type 4: image à haute résolution avec nuances de gris***

6. ***Enregistrement logique de type 9: points caractéristiques***

7. ***Enregistrement logique de type 13: image de trace latente à résolution variable***

8. ***Enregistrement logique de type 15: images d'empreintes palmaires à résolution variable***

9. ***Appendices au chapitre 2 (échange de données dactyloscopiques)***

9.1. *Codes de séparation ASCII*

9.2. *Calcul du caractère de contrôle alphanumérique*

9.3. *Codage de caractères*

9.4. *Résumé des opérations*

9.5. *Définition des enregistrements de type 1*

9.6. *Définition des enregistrements de type 2*

9.7. *Codes des algorithmes de compression (images à niveaux de gris)*

9.8. *Spécifications pour le courrier électronique*

CHAPITRE 3: **Échange de données relatives à l'immatriculation des véhicules**

1. ***Ensemble commun de données aux fins de la consultation automatisée de données relatives à l'immatriculation des véhicules***

1.1. *Définitions*

1.2. *Recherche concernant un véhicule, un propriétaire ou un détenteur*

2. ***Sécurité des données***

2.1. *Aperçu*

2.2. *Caractéristiques de sécurité liées à l'échange de messages*

2.3. *Caractéristiques de sécurité non liées à l'échange de messages*

3. ***Conditions techniques de l'échange de données***

3.1. *Description générale de l'application Eucaris*

3.2. *Exigences fonctionnelles et non fonctionnelles*

CHAPITRE 4: **Évaluation**

1. ***Procédure d'évaluation en vertu de l'article 20 (préparation des décisions conformément à l'article 25, paragraphe 2, de la décision 2008/615/JAI)***

1.1. *Questionnaire*

1.2. *Essai en conditions réelles*

1.3. *Visite d'évaluation*

1.4. *Rapport au Conseil*

2. ***Procédure d'évaluation conformément à l'article 21***

2.1. *Statistiques et rapport*

2.2. *Révision*

3. ***Réunion d'experts***

CHAPITRE 1: **Échange de données ADN**

1. ***Questions de criminalistique et règles et algorithmes de concordance dans le domaine génétique***

1.1. *Propriétés des profils ADN*

Le profil ADN peut comprendre 24 paires de nombres représentant les allèles des 24 loci également utilisés dans les procédures d'Interpol en la matière. Le nom de ces loci figure dans le tableau ci-après:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amélogénine
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

Les 7 loci grisés, au premier rang, constituent à la fois l'actuel ensemble européen de référence (European Standard Set of Loci, ESS) et le groupe standard de loci d'Interpol (Interpol Standard Set of Loci, ISSOL).

Règles d'inclusion:

Les profils ADN mis à disposition par les États membres à des fins de consultation et de comparaison, ainsi que les profils ADN transmis aux mêmes fins, doivent comporter au moins 6 loci complètement renseignés ([1]) et peuvent en comprendre d'autres, ou des blancs, en fonction des disponibilités. Les profils ADN de référence doivent comporter au moins 6 des 7 loci de l'ESS. Pour affiner la précision des concordances, tous les allèles disponibles sont stockés dans la base de données des profils ADN indexés et exploités aux fins des consultations et des comparaisons. Il conviendrait que chaque État membre mette en œuvre, aussi rapidement que possible en pratique, tout nouvel ESS adopté par l'Union européenne.

Il est interdit d'inclure des profils obtenus à partir d'échantillons mélangés, de sorte que les valeurs alléliques de chaque locus consisteront en deux nombres seulement, lesquels peuvent d'ailleurs être identiques, en cas d'homozygotie sur un locus spécifique.

Les règles ci-après s'appliquent aux caractères de remplacement (ou joker) et aux microvariants:

— toute valeur non numérique figurant dans le profil (par exemple «o», «f», «r», «na», «nr» ou «un»), à l'exception de celle correspondant à l'amélogénine, doit être convertie automatiquement en un caractère de remplacement (*) pour l'exportation et faire l'objet d'une comparaison globale,

— les valeurs numériques «0», «1» ou «99» contenues dans le profil doivent être converties automatiquement en un caractère de remplacement (*) pour l'exportation et faire l'objet d'une comparaison avec tous les autres,

— si 3 allèles sont fournis pour un locus, le premier sera accepté et les deux autres devront être automatiquement convertis en un caractère générique (*) pour l'exportation et faire l'objet d'une comparaison globale,

— lorsqu'une valeur de remplacement est fournie pour l'allèle 1 ou l'allèle 2, les deux permutations de la valeur numérique donnée pour le locus feront l'objet d'une recherche (par exemple 12, * pourrait concorder avec 12,14 ou 9,12),

— les microvariants pentanucléotidiques (Penta D, Penta E et CD 4) seront comparés selon le schéma suivant:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x.4

  x.4 = x.2, x.3, x + 1

— les microvariants tétranucléotidiques (le reste des loci sont des tétranucléotides) seront comparés selon le schéma suivant:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x + 1

([1]) Les termes «complètement renseignés» signifient que le traitement des valeurs alléliques rares est inclus.

1.2. *Règles de concordance*

Deux profils génétiques seront comparés à partir des loci pour lesquels une paire de valeurs alléliques est disponible dans les deux profils. Il doit y avoir concordance entre au moins 6 loci complets désignés (à l'exclusion de l'amélogénine) des deux profils ADN pour qu'une réponse indiquant l'existence d'une concordance soit fournie.

Une concordance complète (qualité 1) est définie comme une concordance lorsque l'ensemble des valeurs alléliques des loci contenus à la fois dans le profil de question et le profil de comparaison sont les mêmes. Une quasi-concordance est définie comme une concordance lorsque la valeur d'un seul de tous les allèles comparés diffère entre les deux profils ADN (qualité 2, 3 et 4). Une quasi-concordance n'est acceptée qu'en cas de concordance entre au moins 6 loci complets désignés des deux profils ADN comparés.

Une telle quasi-concordance peut-être due à:

— une faute de frappe dans l'un des profils ADN, dans la demande de consultation ou dans la base de données ADN,

— une erreur de détermination ou de désignation de l'allèle lors de l'établissement d'un profil ADN.

1.3. *Règles en matière de rapports*

Tant les concordances complètes que les quasi-concordances et les cas où il n'y a «pas de concordance» devront faire l'objet d'un rapport.

Les rapports de concordance seront adressés au point de contact national requérant et mis à la disposition du point de contact national requis (afin qu'il puisse évaluer la nature et le nombre des éventuelles demandes de suivi visant à obtenir d'autres données à caractère personnel disponibles et d'autres informations relatives au profil ADN correspondant à la concordance, conformément aux articles 5 et 10 de la décision 2008/615/JAI).

2. ***Tableau des codes des États membres***

Conformément à la décision 2008/615/JAI, les codes de la norme ISO 3166-1 alpha-2 sont utilisés pour attribuer les noms de domaine et définir les autres paramètres de configuration des applications d'échange de données ADN en réseau fermé créées en application du traité de Prüm.

La norme ISO 3166-1 alpha-2 prévoit les codes à deux lettres ci-après pour les États membres:

État membre	Code	État membre	Code
Belgique	BE	Luxembourg	LU
Bulgarie	BG	Hongrie	HU
République tchèque	CZ	Malte	MT
Danemark	DK	Pays-Bas	NL
Allemagne	DE	Autriche	AT
Estonie	EE	Pologne	PL
Grèce	EL	Portugal	PT
Espagne	ES	Roumanie	RO
France	FR	Slovaquie	SK
Irlande	IE	Slovénie	SI
Italie	IT	Finlande	FI
Chypre	CY	Suède	SE
Lettonie	LV	Royaume-Uni	UK
Lituanie	LT		

3. ***Analyse fonctionnelle***

3.1. *Disponibilité du système*

Il conviendrait que les demandes formulées conformément à l'article 3 de la décision 2008/615/JAI soient soumises à la base de données concernée dans l'ordre chronologique de l'envoi de chaque demande, alors que les réponses devraient être transmises de façon qu'elles parviennent à l'État membre requérant dans les quinze minutes qui suivent l'arrivée des demandes.

3.2. *Deuxième étape*

Lorsqu'un État membre reçoit un rapport indiquant l'existence d'une concordance, il incombe à son point de contact national de comparer les valeurs figurant dans le profil ayant fait l'objet de la demande et celles du ou des profils reçus en réponse, afin de valider et de vérifier la valeur probante du profil. Les points de contact nationaux peuvent entrer en communication les uns avec les autres aux fins de la validation.

Les procédures relatives à l'entraide judiciaire démarrent après la validation d'une concordance entre deux profils, sur la base d'un rapport de concordance complète ou de quasi-concordance obtenu pendant la phase de consultation automatisée.

4. ***Document de contrôle des interfaces ADN***

4.1. *Introduction*

4.1.1. Objectifs

La présente partie définit les prescriptions en matière d'échange d'informations relatives aux profils ADN entre les bases de données génétiques de l'ensemble des États membres. Les champs d'en-tête sont spécifiquement définis pour l'échange de données ADN en application du traité de Prüm, alors que les champs de données sont fondés sur la partie correspondant aux données du profil ADN, dans le schéma XML défini pour la passerelle ADN d'Interpol.

Les données sont échangées au moyen du protocole SMTP (Simple Mail Transfer Protocol) ou d'autres techniques modernes, par l'intermédiaire d'un serveur central de messagerie électronique mis en place par le fournisseur de réseau. Le fichier XML est transmis dans le corps d'un message.

4.1.2. Champ d'application

Le présent document de contrôle des interfaces ne définit que le corps des messages électroniques. Tous les aspects qui concernent spécifiquement le réseau et la messagerie électronique sont définis d'une façon uniforme afin de prévoir une base technique commune pour l'échange de données ADN.

Ce cadre commun:

— prévoit une définition du format du champ «objet» du message, afin de permettre un traitement automatisé des messages,

— précise s'il y a lieu de crypter le contenu et, le cas échéant, quelles méthodes doivent être utilisées,

— fixe la longueur maximale des messages.

4.1.3. Principes et structure XML

Le message XML est structuré comme suit:

— en-tête, contenant des informations sur la transmission, et

— données, contenant des informations propres au profil, ainsi que le profil lui-même.

Le même schéma XML est utilisé tant pour la demande que pour la réponse.

Pour pouvoir procéder à des vérifications complètes des profils ADN non identifiés (article 4 de la décision 2008/615/JAI), il doit être possible d'envoyer une série de profils dans un seul message. Il faut fixer un nombre maximal de profils pouvant être inclus dans un même message. Ce nombre dépend de la taille maximale autorisée des messages électroniques et sera fixé une fois que le serveur de messagerie électronique aura été sélectionné.

Exemple de code XML:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

[…]

</header>

<datas>

[…]

</datas>

[<datas> structure «datas» répétée si plus d'un profil est envoyé (….) dans un même message SMTP, uniquement dans les cas visés à l'article 4

</datas>]

</PRUEMDNA>

4.2. *Définition de la structure XML*

Les définitions qui suivent sont présentées à titre documentaire et pour faciliter la lecture. Les informations réellement obligatoires sont définies dans un fichier de schéma XML (PRUEM DNA.xsd).

4.2.1. Schéma PRUEMDNAx

Il comprend les champs ci-après:

Champ	Type	Description
header	PRUEM_header	Nombre: 1
datas	PRUEM_datas	Nombre: 1 … 500

4.2.2. Contenu de l'en-tête

4.2.2.1. PRUEM_header

Il s'agit d'une structure décrivant l'en-tête du fichier XML. Elle comprend les champs ci-après:

Champ	Type	Description
direction	PRUEM_header_dir	Direction de circulation du message
ref	String (chaîne de caractères)	Référence au ficher XML
generator	String (chaîne de caractères)	Créateur du fichier XML
schema_version	String (chaîne de caractères)	Numéro de version du schéma à utiliser
requesting	PRUEM_header_info	Informations relatives à l'État requérant
requested	PRUEM_header_info	Informations relatives à l'État requis

4.2.2.2. PRUEM_header dir

Type des données contenues dans le message. La valeur peut être:

Valeur	Description
R	Demande (Request)

Valeur	Description
A	Réponse (Answer)

4.2.2.3. PRUEM_header_info

Structure permettant de décrire l'État membre ainsi que la date et l'heure de la création du message. Cette structure comprend les champs ci-après:

Champ	Type	Description
source_isocode	String (chaîne de caractères)	Code ISO 3166-2 de l'État membre requérant
destination_isocode	String (chaîne de caractères)	Code ISO 3166-2 de l'État membre requis
request_id	String (chaîne de caractères)	Identifiant unique d'une demande
date	Date	Date de la création d'un message
time	Time (heure)	Heure de la création d'un message

4.2.3. Contenu des profils de données PRUEM

4.2.3.1. PRUEM_datas

Il s'agit d'une structure décrivant la partie des données XML concernant le profil. Elle comprend les champs suivants:

Champ	Type	Description
reqtype	PRUEM_request_type	Type de demande (article 3 ou 4)
date	Date	Date de stockage du profil
type	PRUEM_datas_type	Type de profil
result	PRUEM_datas_result	Résultat de la demande
agency	String (chaîne de caractères)	Nom de l'unité correspondante responsable du profil
profile_ident	String (chaîne de caractères)	Identifiant unique de profil d'État membre
message	String (chaîne de caractères)	Message d'erreur si le résultat = E
profile	IPSG_DNA_profile	Si direction = A (réponse) ET résultat ≠ H (concordance) vide
match_id	String (chaîne de caractères)	En cas de HIT PROFILE_ID du profil requérant
quality	PRUEM_hitquality_type	Qualité de la concordance
hitcount	Integer (entier)	Nombre d'allèles faisant l'objet de la concordance
rescount	Integer (entier)	Nombre de profils faisant l'objet de la concordance. Si la direction = R (demande), alors champ vide. Si la qualité! = 0 (profil original requis), alors champ vide.

4.2.3.2. PRUEM_request_type

Type de données contenues dans le message. Les valeurs peuvent être les suivantes:

Valeur	Description
3	Demandes au titre de l'article 3 de la décision 2008/615/JAI
4	Demandes au titre de l'article 4 de la décision 2008/615/JAI

4.2.3.3. PRUEM_hitquality_type

Valeur	Description
0	Concerne le profil requérant original: S'il n'y a «pas de concordance»: le profil requérant original est renvoyé seul. S'il y a «concordance»: le profil requérant original est renvoyé avec les profils ayant fait l'objet de la concordance.
1	Identique pour tous les allèles disponibles, sans caractères génériques
2	Identique pour tous les allèles disponibles, avec caractères génériques
3	Concordance moyennant déviation (microvariant)
4	Concordance avec non-concordance

4.2.3.4. PRUEM_data_type

Type de données contenues dans le message. Les valeurs peuvent être les suivantes:

Valeur	Description
P	Profil d'une personne
S	Trace (Stain)

4.2.2.5. PRUEM_data_result

Type de données contenues dans le message. Les valeurs peuvent être les suivantes:

Valeur	Description
U	Indéfini (Undefined), si direction = R (demande)
H	Concordance (Hit)
N	Pas de concordance (Non Hit)
E	Erreur

4.2.3.6. IPSG_DNA_profile

Structure décrivant un profil ADN. Elle contient les champs suivants:

Champ	Type	Description
ess_issol	IPSG_DNA_ISSOL	Groupe de loci correspondant à l'ISSOL (groupe standard de loci d'Interpol)
additional_loci	IPSG_DNA_additional_loci	Autres loci
marker	String (chaîne de caractères)	Méthode utilisée pour générer l'ADN
profile_id	String (chaîne de caractères)	Identifiant unique du profil ADN

4.2.3.7. IPSG_DNA_ISSOL

Structure contenant les loci ISSOL (groupe standard de loci d'Interpol). Elle comporte les champs suivants:

Champ	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Champ	Type	Description
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amélogénine

4.2.3.8. IPSG_DNA_additional_loci

Structure contenant les autres loci. Elle comporte les champs suivants:

Champ	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Structure décrivant un locus. Elle comporte les champs suivants:

Champ	Type	Description
low_allele	String (chaîne de caractères)	Valeur la plus basse d'un allèle
high_allele	String (chaîne de caractères)	Valeur la plus élevée d'un allèle

5. ***Application, sécurité et architecture de communication***

5.1. *Présentation*

Pour la mise en œuvre d'applications aux fins de l'échange de données ADN dans le cadre de la décision 2008/615/JAI, un réseau de communication fermé sera mis en place à l'usage exclusif des États membres. Pour tirer parti de cette infrastructure commune de communication et envoyer les demandes et recevoir les réponses d'une

façon plus efficace, un mécanisme asynchrone a été retenu pour transmettre les demandes de données ADN et dactyloscopiques dans un message électronique transmis via le protocole SMTP. Pour des raisons de sécurité, on aura recours à la norme S/MIME (Secure Multipurpose Internet Mail Extensions, ou MIME sécurisé), qui étend les fonctionnalités du protocole SMTP, afin d'établir un véritable tunnel sécurisé de bout en bout sur le réseau.

Le réseau de communication opérationnel TESTA (Services télématiques transeuropéens sécurisés entre administrations) est utilisé pour l'échange de données entre États membres. TESTA relève de la responsabilité de la Commission européenne. Comme les bases de données ADN nationales et les points d'accès nationaux actuels à TESTA peuvent se trouver sur différents sites dans les États membres, il peut exister deux modes d'accès à TESTA:

1) soit en utilisant les points d'accès nationaux existants ou en établissant un nouveau point d'accès TESTA;

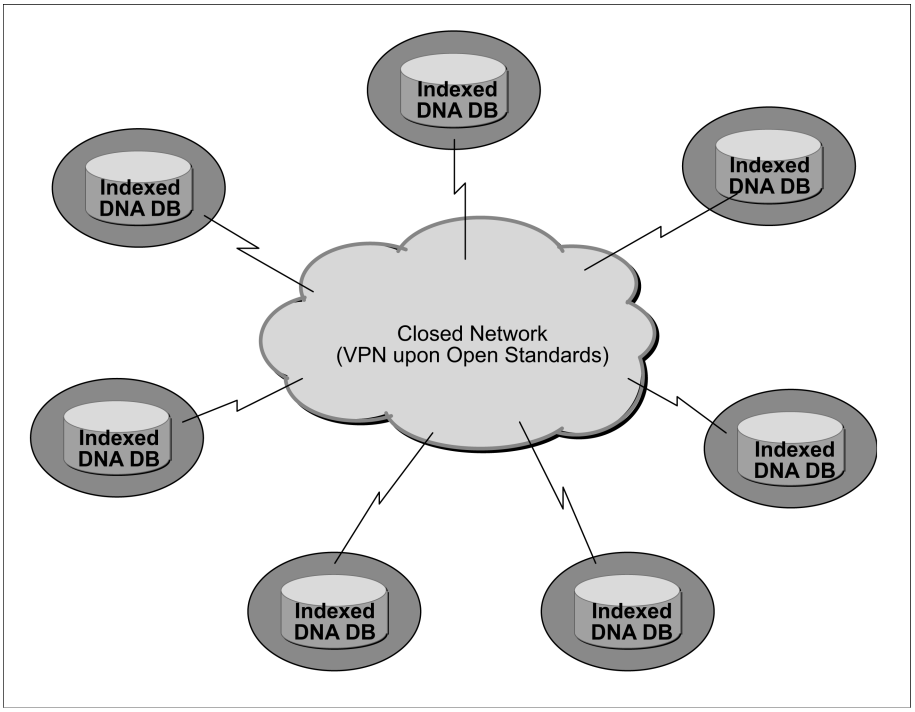
2) soit en créant un lien local sécurisé entre le site où se trouve la base de données ADN et le point d'accès national TESTA existant, ce lien étant administré par le service national compétent.

Les protocoles et les normes utilisés pour la mise en œuvre des applications prévues dans le cadre de la décision 2008/615/JAI sont conformes aux standards ouverts et aux exigences imposées par les autorités chargées de l'élaboration de la politique des États membres en matière de sécurité.

5.2. *Architecture de haut niveau*

La décision 2008/615/JAI prévoit que chaque État membre met ses données ADN à disposition des autres États membres, conformément au format commun standardisé, à des fins d'échange et/ou de consultation. L'architecture se fonde sur le modèle de communication «de point à point». Il n'existe ni serveur informatique centralisé ni base de données unique contenant des profils ADN.

Figure 1: topologie de l'échange de données ADN



Outre le respect des contraintes juridiques nationales, chaque État membre doit décider du type de matériel et de logiciel devant être déployé pour que la configuration mise en œuvre sur son site respecte les exigences de la décision 2008/615/JAI.

5.3. *Normes de sécurité et protection des données*

Trois niveaux de sécurité ont été envisagés et mis en œuvre.

5.3.1. Niveau des données

Les données relatives aux profils ADN fournies par chaque État membre doivent être préparées conformément à une norme commune de protection des données, de sorte qu'un État membre requérant reçoive une réponse indiquant essentiellement l'existence ou l'absence d'une concordance, ainsi qu'un numéro d'identification en cas de concordance, sans aucune information à caractère personnel. Les recherches complémentaires, après notification d'une concordance, seront menées au niveau bilatéral, conformément aux instruments nationaux applicables aux sites de chacun des États membres en matière juridique et organisationnelle.

5.3.2. Niveau de la communication

Avant d'être transmis vers les sites des autres États membres, les messages contenant des informations sur les profils ADN (demandes et réponses) seront cryptés au moyen d'un système moderne conforme aux standards ouverts, par exemple le protocole S/MIME.

5.3.3. Niveau de la transmission

Tous les messages cryptés contenant des informations relatives à des profils ADN seront envoyés vers les sites des autres États membres via un système de réseau privé virtuel, administré par un fournisseur de réseau de confiance au niveau international. Les accès sécurisés à ce réseau privé relèveront de la responsabilité nationale. Ce système de réseau privé virtuel n'est pas relié à l'internet.

5.4. *Protocoles et normes à mettre en œuvre pour le cryptage: S/MIME et mécanismes connexes*

Le standard ouvert S/MIME, qui étend les fonctionnalités du protocole SMTP, norme de facto pour la messagerie électronique, sera déployé pour crypter les messages contenant des informations relatives à des profils ADN. Le protocole S/MIME (v. 3), qui prévoit des confirmations signées, des étiquettes de sécurité et des listes de diffusion sécurisées, est organisé en couches selon la spécification de l'Internet Engineering Task Force (IETF) pour la protection cryptographique des messages, à savoir la Cryptographic Message Syntax (CMS). Il peut être utilisé pour signer, résumer, authentifier ou crypter numériquement les données numériques sous toutes leurs formes.

Le certificat sous-jacent utilisé par le mécanisme S/MIME doit être conforme à la norme X.509. Pour garantir l'uniformité des normes et des procédures avec les autres applications déployées dans le cadre du traité de Prüm, les règles de traitement des opérations de cryptage S/MIME ou à appliquer par les diverses plates-formes du commerce sont les suivantes:

— la séquence des opérations est: d'abord cryptage, puis signature,

— on appliquera les algorithmes de cryptage AES (Advanced Encryption Standard) avec une clé de 256 bits, et RSA (Rivest Shamir Adleman) avec une clé de 1 024 bits, respectivement aux cryptages symétriques et asymétriques,

— la fonction de hachage cryptographique SHA-1 sera appliquée.

La fonctionnalité S/MIME est intégrée dans la grande majorité des logiciels modernes de messagerie électronique, notamment Outlook, Mozilla Mail et Netscape Communicator 4.x, et est capable d'interopérer avec tous les principaux logiciels de messagerie.

Le protocole S/MIME pouvant être facilement intégré dans les infrastructures informatiques nationales, dans tous les sites des États membres, il a été choisi comme mécanisme viable de mise en œuvre de la sécurité au niveau de la communication. Pour valider cette approche d'une façon plus efficace et réduire les coûts, l'interface de programmation (API) JavaMail, qui est un standard ouvert, est retenue pour le prototypage de l'échange des données ADN. L'API JavaMail prévoit un processus simple de cryptage et de décryptage des courriels, grâce aux normes S/MIME et/ou OpenPGP. Le but est de disposer d'une interface de programmation unique et d'utilisation simple pour les clients de messagerie avec lesquels on souhaite envoyer et recevoir des messages cryptés avec les deux méthodes les plus utilisées. C'est pourquoi toute implémentation moderne de l'API JavaMail suffira pour satisfaire aux exigences visées par la décision 2008/615/JAI, par exemple, l'interface JCE (Java Cryptographic Extension) de BouncyCastle, qui sera utilisée pour la mise en œuvre du protocole S/MIME aux fins du prototypage de l'échange de données ADN entre l'ensemble des États membres.

5.5. *Architecture de l'application*

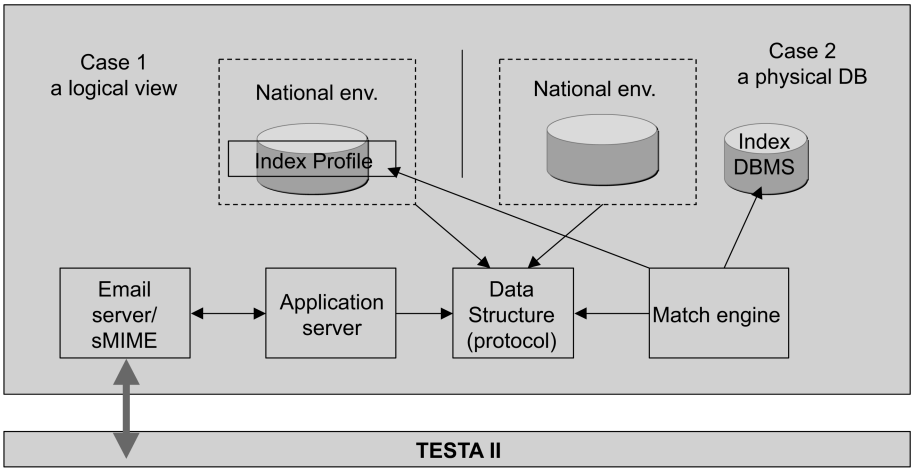
Chaque État membre fournira aux autres États membres un ensemble de données normalisées relatives à des profils ADN conformes à la version actuelle du document commun de contrôle des interfaces. Pour ce faire, on peut soit créer une vue logique à partir de la base de données nationale, soit créer une base de données alimentée par exports (base de données indexée).

Les quatre composantes principales (serveur de messagerie et protocole S/MIME, serveur d'applications, zone de structure des données pour extraire et ajouter des données et enregistrer les messages entrants et sortants, et moteur de concordance) appliquent l'ensemble de la logique de l'application indépendamment du produit.

Pour que tous les États membres puissent intégrer facilement les composantes dans leurs sites nationaux, la fonctionnalité commune spécifiée a été mise en œuvre au moyen de composantes de logiciels libres, qui pourraient être sélectionnées par chaque État membre en fonction de la politique et de la réglementation applicables au niveau national en matière informatique. Étant donné que des fonctions distinctes doivent être mises en œuvre pour accéder aux bases de données indexées contenant des profils ADN couverts par la décision 2008/615/JAI, il est loisible à chaque État membre de choisir sa plate-forme matérielle et logicielle, y compris la base de données et le système d'exploitation.

Un prototype pour l'échange de données ADN a été élaboré et testé avec succès sur le réseau commun existant. La version 1.0 a été déployée en production et est utilisée pour les opérations quotidiennes. Les États membres peuvent recourir au produit mis au point en commun mais peuvent aussi développer leurs propres produits. Les composantes du produit commun seront entretenues, adaptées et enrichies en fonction de l'évolution des besoins en matière informatique, criminalistique et/ou de police opérationnelle.

Figure 2: Aperçu topologique de l'application



5.6. *Protocoles et normes à utiliser dans l'architecture de l'application*

5.6.1. XML

L'échange de données ADN tirera pleinement parti d'un schéma XML en pièce jointe à des messages électroniques utilisant le protocole SMTP. Le XML (EXtensible Markup Language) est un langage de balisage polyvalent, recommandé par le Consortium World Wide Web (W3C) et utilisé pour créer des langages de balisage spécialisés permettant de décrire de nombreux types différents de données. La description d'un profil ADN susceptible d'être échangée entre l'ensemble des États membres repose sur le langage XML et sur un schéma XML figurant dans le document de contrôle des interfaces.

5.6.2. ODBC

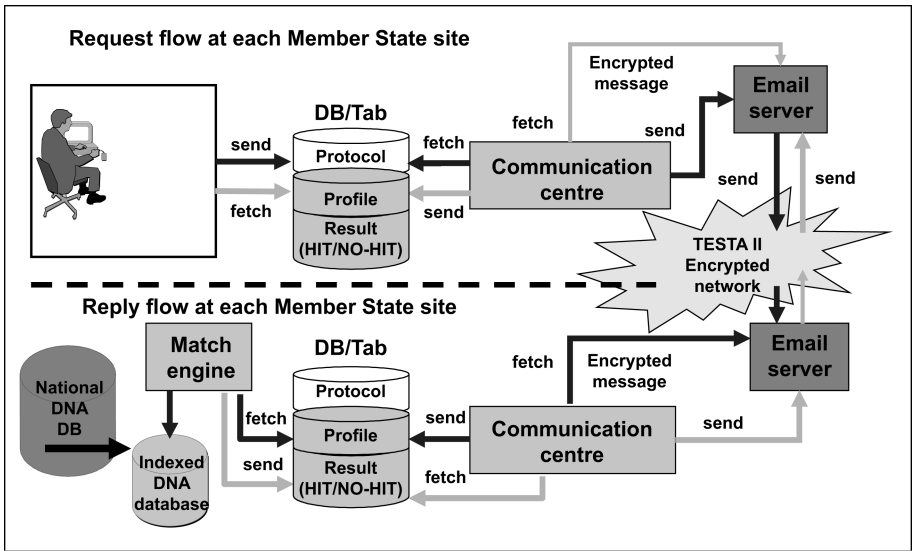
La norme ODBC (Open DataBase Connectivity) propose une interface de programmation normalisée permettant d'accéder à des systèmes de gestion de bases de données (SGBD); l'interface est indépendante des langages de programmation, des bases de données et des systèmes d'exploitation. La norme ODBC a toutefois ses inconvénients. L'administration d'un grand nombre de clients peut nécessiter la mise en œuvre de pilotes et de bibliothèques de liens dynamiques (DLL) très divers. Cette complexité peut se traduire par des surcoûts en matière d'administration des systèmes.

5.6.3. JDBC

JDBC (Java DataBase Connectivity) est une interface de programmation pour le langage JAVA, qui définit de quelle manière un client accède à une base de données. Contrairement à la norme ODBC, l'API JDBC se passe de bibliothèques dynamiques locales installées sur l'ordinateur de bureau.

La logique du traitement des demandes et des réponses relatives aux profils ADN, dans les sites de chaque État membre, est décrite dans le diagramme ci-dessous. Les flux de demandes et de réponses interagissent avec une zone de données neutre comprenant divers ensembles de données partageant une même structure.

Figure 3: Aperçu du déroulement des opérations dans les sites des États membres



5.7. *Cadre de communication*

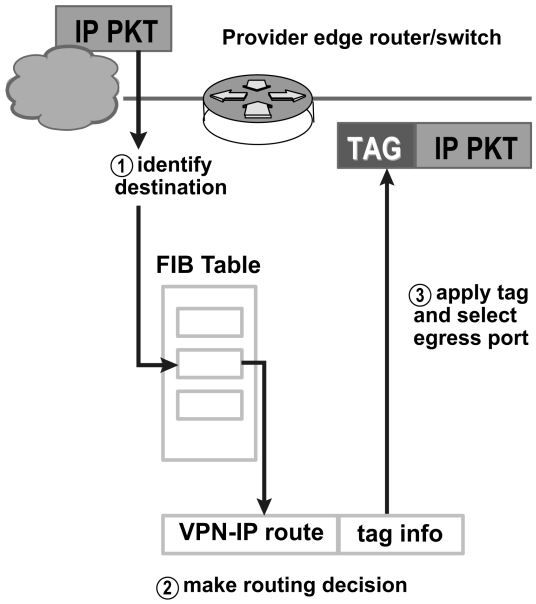
5.7.1. Réseau commun de communication: TESTA et son infrastructure de suivi

L'application d'échange des données ADN tirera parti de la messagerie électronique, un mécanisme asynchrone, pour l'envoi des demandes et la réception des réponses entre les États membres. Comme l'ensemble des États membres dispose d'au moins un point d'accès national au réseau TESTA, l'échange des données ADN passera par ce réseau. TESTA offre plusieurs services appréciables par le biais de son serveur de messagerie électronique. Outre qu'elle héberge les boîtes aux lettres électroniques spécifiques de TESTA, cette infrastructure permet de créer des listes de distribution de courrier électronique ainsi que des règles de routage. Il est ainsi possible de recourir à TESTA en tant que plaque tournante pour les messages adressés aux administrations reliées à des domaines couvrant l'ensemble de l'Union européenne. Il est également possible de mettre en place des mécanismes de protection contre les virus.

Le serveur de messagerie de TESTA repose sur une plate-forme matérielle à disponibilité élevée, qui est localisée dans les installations centrales du réseau et protégée par un pare-feu. Le système de noms de domaine (DNS, pour Domain Name System) de TESTA établit une correspondance entre les adresses universelles (URL) et les adresses IP et isole l'utilisateur et les applications des questions liées à la résolution des adresses.

5.7.2. Questions de sécurité

Le concept de réseau privé virtuel (VPN, pour Virtual Private Network) a été mis en œuvre dans le cadre de TESTA. La technologie de commutation de balises utilisée pour la mise en place de ce réseau privé virtuel sera mise en conformité avec la norme multiprotocoles de commutation d'étiquettes (MPLS, pour Multiprotocol Label Switching) conçue par l'IETF (Internet Engineering Task Force).



La technologie MPLS est une norme mise au point par l'IETF, qui permet d'accélérer le trafic sur le réseau en évitant l'analyse des paquets par les routeurs intermédiaires. À cet effet, des «étiquettes» sont jointes aux paquets par les routeurs situés aux deux extrémités de la dorsale, en fonction d'informations contenues dans une table de routage (FIB, pour Forwarding Information Base). Ses étiquettes sont également utilisées pour la mise en œuvre des réseaux privés virtuels (VPN).

La technologie MPLS combine les avantages du routage (couche 3) et ceux de la commutation (couche 2). Les adresses IP n'étant pas analysées au cours de la transmission sur la dorsale, la technologie MPLS n'impose aucune limitation sur l'adressage IP.

En outre, les courriers électroniques transmis par le réseau TESTA seront protégés par le mécanisme de cryptage fondé sur le protocole S/MIME. Il est impossible pour qui que ce soit de déchiffrer les messages transmis par ce réseau sans la clé et le certificat approprié.

5.7.3. Protocoles et normes à utiliser sur le réseau de communication

5.7.3.1. SMTP

Le protocole SMTP (Simple Mail Transfer Protocol) est la norme de facto pour la transmission du courrier électronique sur l'internet. Le protocole SMTP est assez simple et recourt à des informations textuelles: le ou les destinataires du message sont spécifiés, puis le corps du message est transmis. Le protocole SMTP utilise le port TCP 25, conformément aux spécifications de l'IETF. L'enregistrement MX (Mail eXchange record) du système de noms de domaines (DNS) est utilisé pour déterminer le serveur SMTP qui correspond à un nom de domaine donné.

Comme ce protocole reposait entièrement, à ses débuts, sur du texte au format ASCII, il n'était pas bien adapté aux fichiers binaires. Des normes telles que le protocole MIME (Multipurpose Internet Mail Extensions) ont été mises au point afin d'encoder les fichiers binaires pour les transmettre par le protocole SMTP. De nos jours, la plupart des serveurs SMTP prennent en charge les extensions 8BITMIME et S/MIME, ce qui permet de transmettre des fichiers binaires presque aussi facilement que du texte brut. Les règles de traitement pour les opérations nécessitant le recours au protocole S/MIME sont décrites dans la partie concernée (voir le point 5.4).

SMTP est un protocole de distribution sélective («push»): il ne permet pas de récupérer à la demande les messages se trouvant sur un serveur distant. Il faut recourir, à cet effet, à un client de messagerie utilisant les protocoles POP3 ou IMAP. Pour l'échange de données ADN, il a été décidé de recourir au protocole POP3.

5.7.3.2. POP

Les clients de messagerie locaux utilisent le Post Office Protocol Version 3 (POP3), un protocole internet normalisé appartenant à la couche applications, pour récupérer des messages électroniques se trouvant sur un serveur distant, par le biais d'une connexion TCP/IP. Les clients de messagerie envoient des messages sur l'internet ou un réseau d'entreprise en recourant au profil «Submit» du protocole SMTP. Le protocole MIME est la norme pour les pièces jointes et le texte non-ASCII contenu dans les messages. Quoique ni le protocole POP3 ni le protocole SMTP n'exigent que les messages soient formatés selon le protocole MIME, la majorité des courriels transitant par l'internet ont ce format, de sorte que les clients POP doivent également prendre en charge et utiliser ce protocole. Par conséquent, l'ensemble de l'environnement de communication prévu par la décision 2008/615/JAI prendra en charge les composantes du protocole POP.

5.7.4. Attribution des adresses de réseau

Environnement opérationnel

Le RIPE (Réseaux IP européens), autorité compétente en Europe pour l'attribution des adresses IP, a alloué à TESTA un bloc d'adresses dédié pour sous-réseau de classe C. Si nécessaire, d'autres blocs d'adresses pourraient, à l'avenir, être alloués à TESTA. En Europe, les adresses IP sont attribuées aux États membres sur une base géographique. L'échange des données entre les États membres, dans le cadre de la décision 2008/615/JAI, se déroule à l'intérieur d'un réseau IP fermé (du point de vue logique) couvrant l'ensemble de l'Europe.

Environnement d'essai

Afin d'assurer le bon fonctionnement de l'environnement au quotidien pour l'ensemble des États membres qui y sont reliés, il faut mettre en place un environnement d'essai dans le réseau fermé, à l'intention des nouveaux États membres qui se disposent à participer aux opérations. Une liste comprenant notamment les adresses IP, les paramètres de configuration du réseau, les domaines de messagerie ainsi que les comptes d'utilisateurs des applications a été dressée et devrait être appliquée sur le site de l'État membre concerné. En outre, un ensemble de faux profils ADN a été constitué à des fins de test.

5.7.5. Paramètres de configuration

Un système de messagerie électronique sécurisé utilisant le domaine eu-admin.net est créé. Ce domaine — et les adresses qui y sont liées — ne sera pas accessible de l'extérieur du domaine TESTA, qui couvre l'ensemble de l'Union européenne, les noms n'étant connus que par le serveur DNS central de TESTA, qui est isolé de l'internet.

La conversion de ces adresses de sites TESTA (nom d'hôtes) en adresses IP est effectuée par le service DNS de TESTA. Pour chaque domaine local, un enregistrement MAIL sera ajouté à ce serveur DNS central de TESTA, ce qui permettra de réexpédier tous les messages électroniques envoyés à des domaines locaux du réseau TESTA vers le serveur central de messagerie de TESTA. Ce serveur central de TESTA les réexpédiera alors vers le serveur de messagerie spécifique du domaine local, en utilisant les adresses électroniques dudit domaine local. Grâce à une telle procédure de réexpédition des messages, les informations sensibles qu'ils contiennent ne transitent que par l'infrastructure de réseau fermée qui couvre l'ensemble de l'Europe, et non par l'internet, qui n'est pas un environnement sûr.

Sur les sites de chaque État membre, il faut créer des sous-domaines (indiqués en caractères ***gras et italiques***) selon la syntaxe qui suit:

«***type-d'-application*.pruem.*code-de-l'État-membre***.eu-admin.net», où:

«***code-de-l'État-membre***» est l'un des codes à deux lettres des États membres (par exemple AT, BE, etc.)

«***type-d'-application***» est l'une des deux valeurs qui suivent: DNA et FP.

Sur la base de la syntaxe décrite ci-dessus, les sous-domaines des États membres sont indiqués dans le tableau qui suit:

EM	Sous-domaines	Notes
BE	***dna*.pruem.be**.eu-admin.net	Création d'un lien local sécurisé vers le point d'accès à TESTA existant
	***fp*.pruem.be**.eu-admin.net	
BG	***dna*.pruem.bg**.eu-admin.net	
	***fp*.pruem.bg**.eu-admin.net	
CZ	***dna*.pruem.cz**.eu-admin.net	
	***fp*.pruem.cz**.eu-admin.net	
DK	***dna*.pruem.dk**.eu-admin.net	
	***fp*.pruem.dk**.eu-admin.net	
DE	***dna*.pruem.de**.eu-admin.net	Utilisation des points d'accès nationaux à TESTA II existants
	***fp*.pruem.de**.eu-admin.net	
EE	***dna*.pruem.ee**.eu-admin.net	
	***fp*.pruem.ee**.eu-admin.net	

EM	Sous-domaines	Notes
IE	***dna*.pruem.ie**.eu-admin.net	
	***fp*.pruem.ie**.eu-admin.net	
EL	***dna*.pruem.el**.eu-admin.net	
	***fp*.pruem.el**.eu-admin.net	
ES	***dna*.pruem.es**.eu-admin.net	Utilisation du point d'accès national à TESTA II existant
	***fp*.pruem.es**.eu-admin.net	
FR	***dna*.pruem.fr**.eu-admin.net	Utilisation du point d'accès national à TESTA II existant
	***fp*.pruem.fr**.eu-admin.net	
IT	***dna*.pruem.it.**eu-admin.net	
	***fp*.pruem.it.**eu-admin.net	
CY	***dna*.pruem.cy.**eu-admin.net	
	***fp*.pruem.cy.**eu-admin.net	
LV	***dna*.pruem.lv.**eu-admin.net	
	***fp*.pruem.lv.**eu-admin.net	
LT	***dna*.pruem.lt.**eu-admin.net	
	***fp*.pruem.lt.**eu-admin.net	
LU	***dna*.pruem.lu**.eu-admin.net	Utilisation du point d'accès national à TESTA II existant
	***fp*.pruem.lu**.eu-admin.net	
HU	***dna*.pruem.hu.**eu-admin.net	
	***fp*.pruem.hu.**eu-admin.net	
MT	***dna*.pruem.mt.**eu-admin.net	
	***fp*.pruem.mt.**eu-admin.net	
NL	***dna*.pruem.nl**.eu-admin.net	Projet de création d'un nouveau point d'accès à TESTA II au Nederlands Forensisch Instituut (NFI)
	***fp*.pruem.nl**.eu-admin.net	
AT	***dna*.pruem.at**.eu-admin.net	Utilisation du point d'accès national à TESTA II existant
	***fp*.pruem.at**.eu-admin.net	
PL	***dna*.pruem.pl.**eu-admin.net	
	***fp*.pruem.pl.**eu-admin.net	
PT	***dna*.pruem.pt**.eu-admin.net	……
	***fp*.pruem.pt**.eu-admin.net	……
RO	***dna*.pruem.ro.**eu-admin.net	
	***fp*.pruem.ro**.eu-admin.net	

EM	Sous-domaines	Notes
SI	***dna*.pruem.si**.eu-admin.net	……
	***fp*.pruem.si**.eu-admin.net	……
SK	***dna*.pruem.sk**.eu-admin.net	
	***fp*.pruem.sk**.eu-admin.net	
FI	***dna*.pruem.fi**.eu-admin.net	*[À insérer]*
	***fp*.pruem.fi**.eu-admin.net	
SE	***dna*.pruem.se**.eu-admin.net	
	***fp*.pruem.se**.eu-admin.net	
UK	***dna*.pruem.uk**.eu-admin.net	
	***fp*.pruem.uk**.eu-admin.net	

CHAPITRE 2: **Échange de données dactyloscopiques (document de contrôle des interfaces)**

L'objet du présent document de contrôle des interfaces est de définir les besoins en ce qui concerne l'échange d'informations dactyloscopiques entre les fichiers automatisés d'empreintes digitales (FAED) des États membres. Il repose sur la norme ANSI/NIST-ITL 1-2000 (INT-I, version 4.22b), telle que mise en œuvre par Interpol.

Cette version couvre l'ensemble des définitions de base des enregistrements logiques de types 1, 2, 4, 9, 13 et 15 nécessaires pour le traitement dactyloscopique fondé sur les images et les points caractéristiques (ou minuties).

1. ***Aperçu de la teneur des fichiers***

Un fichier dactyloscopique se compose de plusieurs enregistrements logiques. La norme ANSI/NIST − ITL1 − 2000 définit seize types d'enregistrements logiques. Chaque enregistrement est séparé du suivant par un séparateur ASCII approprié. Il en va de même à l'intérieur des enregistrements, pour chaque zone et chaque sous-zone.

Seuls six types d'enregistrements sont utilisés pour l'échange d'informations entre l'agence expéditrice et l'agence destinataire:

Type 1 → en-tête de fichier
Type 2 → descriptif
Type 4 → image à haute résolution avec nuances de gris
Type 9 → points caractéristiques
Type 13 → image de trace latente à résolution variable
Type 15 → images d'empreintes palmaires à résolution variable

1.1. *Type 1 — en-tête de fichier*

L'enregistrement «en-tête de fichier» contient des informations relatives au routage du message et des indications sur la structure du reste du fichier. Il définit également le type d'opération, qui peut appartenir à l'une des grandes catégories décrites ci-après.

1.2. *Type 2 — descriptif (défini par l'utilisateur)*

L'enregistrement «descriptif» contient diverses informations textuelles intéressant le service expéditeur et le service destinataire.

1.3. *Type 4 — image à haute résolution avec nuances de gris*

Ce type d'enregistrement est utilisé pour la transmission d'images dactyloscopiques à haute résolution avec niveaux de gris (valeurs exprimées sur huit bits), scannées à une résolution de 500 pixels par pouce. Les images dactyloscopiques seront compressées au moyen de l'algorithme WSQ, le rapport de compression ne dépassant pas 15:1. Il convient de ne pas utiliser d'autre algorithme de compression ni d'image non compressée.

1.4. *Type 9 — points caractéristiques*

L'enregistrement de type 9 sert à transmettre des informations sur les lignes ou les points caractéristiques, en partie dans le but d'éviter la répétition des calculs de codes FAED et en partie afin de transmettre des codes plutôt que des images, les codes étant moins «volumineux» que les images correspondantes.

1.5. *Type 13 — image de trace latente à résolution variable*

Cet enregistrement est utilisé pour échanger des images à résolution variable de traces latentes de doigts et de paumes, ainsi que du texte. Les images doivent être numérisées à une résolution de 500 ppp et comporter 256 niveaux de gris. Si l'image est de bonne qualité, elle doit être compressée au moyen de l'algorithme WSQ. Au besoin, l'image peut être améliorée au-delà de 500 ppp et des 256 niveaux de gris prévus, sur accord bilatéral. Dans ce cas, il est fortement recommandé d'utiliser le format JPEG 2000 (voir l'appendice 7).

1.6. *Type 15 — image d'empreinte palmaire à résolution variable*

L'enregistrement de type 15 est utilisé pour échanger des images d'empreintes palmaires à résolution variable, ainsi que du texte. Les images doivent être numérisées à 500 ppp et comporter 256 niveaux de gris. Toutes les images d'empreintes palmaires doivent être compressées au moyen de l'algorithme WSQ, ce qui permet de réduire le volume de données. Au besoin, l'image peut être améliorée au-delà de 500 ppp et des 256 niveaux de gris prévus, sur accord bilatéral. Dans ce cas, il est fortement recommandé d'utiliser le format JPEG 2000 (voir l'appendice 7).

2. ***Format des enregistrements***

Un fichier d'opération comprend un ou plusieurs enregistrements logiques. Chaque enregistrement logique se compose d'une ou de plusieurs zones compatibles avec le type de l'enregistrement. Chaque zone peut contenir un ou plusieurs éléments d'information dont on spécifie la valeur (une seule). C'est l'ensemble des éléments d'information dont se compose une zone qui définissent la valeur de celle-ci. Une zone peut également contenir un ou plusieurs éléments d'information regroupés et répétés un certain nombre de fois. Un tel groupe d'informations est appelé «sous-zone». Une zone peut donc comporter plusieurs sous-zones.

2.1. *Les séparateurs*

En ce qui concerne les enregistrements logiques à zones balisées, les séparateurs utilisés sont les quatre séparateurs ASCII. Ces codes peuvent servir à délimiter les éléments d'information figurant dans une zone ou dans une sous-zone, les zones elles-mêmes ou les multiples occurrences des sous-zones. Ils sont définis dans la norme ANSI X3.4. Ils servent à délimiter et à qualifier logiquement les informations. Il s'agit, par ordre d'importance, du séparateur de fichier FS («File Separator»), du séparateur de groupe GS («Group Separator»), du séparateur d'enregistrement RS («Record Separator») et du séparateur d'unité US («Unit Separator»). On trouvera dans le tableau 1 ci-après le récapitulatif de l'utilisation de ces codes dans le cadre de la présente norme.

Les séparateurs donnent une indication sur le type de données qui les suivent. Le séparateur US sépare des éléments d'information à l'intérieur d'une zone ou d'une sous-zone; il signale que l'élément d'information suivant appartient à cette zone ou sous-zone. Le séparateur RS sépare des sous-zones; sa présence signale le début d'un énième élément d'information répété. Le séparateur GS sépare des zones d'enregistrement; il signale le début d'une autre zone avant le numéro d'identification de zone. De même, le séparateur FS signale le début d'un autre enregistrement logique.

Ces quatre codes n'ont de signification que lorsqu'ils sont utilisés comme séparateurs dans du texte ASCII. Ils n'ont aucune signification dans des enregistrements ou dans des zones binaires; ils font alors partie des données échangées.

Une zone ou un élément d'information ne doit normalement pas être vide. Par conséquent, on ne doit trouver qu'un séparateur entre deux éléments d'information. Les exceptions à cette règle sont les cas où les données sont indisponibles, manquantes ou facultatives, et que le traitement de l'opération concernée ne dépend pas de la présence de ces données. Dans ces cas, on trouvera plusieurs séparateurs côte à côte au lieu de données fictives entre des séparateurs.

Pour la définition d'une zone comportant trois éléments d'information, on appliquera ce qui suit. Si les données manquent pour spécifier le deuxième élément d'information, on aura deux séparateurs US entre le premier et le troisième élément d'information. Si les données manquent pour spécifier le deuxième et le troisième éléments d'information, il faudra introduire trois séparateurs: deux séparateurs US plus le séparateur indiquant la fin de la zone ou de la sous-zone. De façon générale, si un ou plusieurs éléments d'information obligatoires ou facultatifs sont indisponibles pour une zone ou une sous-zone, il faut introduire le nombre voulu de séparateurs.

Il est possible de trouver côte à côte plusieurs combinaisons de deux ou plus des quatre séparateurs utilisables. Lorsque des données sont manquantes ou indisponibles pour un élément d'information, une sous-zone ou une zone d'enregistrement logique, il doit y avoir un séparateur de moins que le nombre d'éléments d'information, de sous-zones ou de zones requis.

Tableau 1: séparateurs utilisés

Code	Type	Fonction	Valeur hexadécimale	Valeur décimale
US	Unit Separator	Sépare des éléments d'information	1F	31
RS	Record Separator	Sépare des sous-zones	1E	30
GS	Group Separator	Sépare des zones	1D	29
FS	File Separator	Sépare des enregistrements logiques	1C	28

2.2. *Format des enregistrements*

En ce qui concerne les enregistrements logiques à zones balisées, chaque zone utilisée doit être numérotée conformément à la présente norme et présenter le format suivant: numéro de type de l'enregistrement logique suivi d'un point (».»), numéro de zone suivi d'un deux-points (»:»), données compatibles avec cette zone. Le numéro de la zone balisée peut être n'importe quel nombre d'un à neuf chiffres, ce numéro devant être placé entre le point et le deux-points. Ce numéro est interprété comme un entier non signé. Cela implique qu'un numéro de zone tel que «2 123:» équivaut au numéro de zone «2.000000123» et est interprété de la même façon.

Dans les exemples donnés tout au long de ce document, on utilisera un nombre à trois chiffres pour désigner les zones contenues dans chacun des enregistrements logiques à zones balisées décrits. Les numéros de zones se présentent sous la forme: «TT.xxx», «TT» représentant le type d'enregistrement à un ou deux caractères suivi d'un point. Les trois caractères suivants correspondent au numéro de zone suivi d'un deux-points. Les caractères ASCII ou les données relatives à l'image arrivent après le deux-points.

Les enregistrements logiques de type 1 et 2 contiennent uniquement des zones de texte ASCII. La première zone ASCII de chacun de ces types d'enregistrement permet d'enregistrer la longueur totale de l'enregistrement (qui prend en compte les numéros de zones, les deux-points et les séparateurs). Le séparateur et caractère de contrôle «FS» (qui marque la fin d'un enregistrement logique ou d'une opération) suit le dernier octet des données ASCII et est pris en compte dans le calcul de la longueur de l'enregistrement.

À la différence des enregistrements à zones balisées, les enregistrements de type 4 ne contiennent que des données binaires enregistrées comme des zones binaires ordonnées à longueur fixe. La longueur totale de l'enregistrement est enregistrée dans la première zone binaire à quatre octets de chaque enregistrement. Pour ces enregistrements binaires, ni le numéro d'enregistrement suivi de son point ni le numéro d'identification de champ et son deux-points ne sont pris en compte. En outre, les longueurs respectives de ces six enregistrements étant soit fixes, soit à spécifier, aucun des quatre séparateurs («US», «RS», «GS» ou «FS») n'est interprété autrement que comme données binaires. En ce qui concerne ces enregistrements binaires, le caractère «FS» ne doit pas être utilisé comme séparateur d'enregistrements ou caractère de fin d'opération.

3. ***Enregistrement logique de type 1: en-tête de fichier***

L'enregistrement «en-tête de fichier» décrit la structure du fichier et en précise le type. Il donne également d'autres informations importantes. Le jeu de caractères utilisé dans l'enregistrement logique de type 1 est uniquement le code ANSI à sept bits pour l'échange d'informations.

3.1. *Les différentes zones de l'enregistrement logique de type 1*

3.1.1. Zone 1.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Cette zone définit le nombre d'octets total de l'enregistrement. Elle commence par «1 001:», suivi de la longueur totale de l'enregistrement, en comptant chaque caractère de chaque zone et les séparateurs.

3.1.2. Zone 1.002: VER (Version Number — numéro de version)

Afin que les utilisateurs sachent sous quelle version de la norme ANSI/NIST ils travaillent, cette zone de quatre octets spécifie le numéro de la version utilisée par le logiciel sous lequel le fichier a été créé ou par le système sur lequel il a été créé. Les deux premiers octets spécifient le numéro de version proprement dit et les deux suivants le numéro de révision: par exemple, la norme 1986 d'origine est considérée comme la première version, spécifiée «0100», et la norme actuelle comme la deuxième version, spécifiée «0300».

3.1.3. Zone 1.003: CNT (File Content — contenu du fichier)

Cette zone contient la liste de tous les enregistrements du fichier, avec leur type et suivant l'ordre dans lequel ils apparaissent dans le fichier logique. Elle peut comporter une ou plusieurs sous-zones. Chaque sous-zone contient deux éléments d'information décrivant un enregistrement logique du fichier. Les sous-zones sont spécifiées suivant l'ordre dans lequel les enregistrements sont enregistrés et transmis.

Le premier élément d'information de la première sous-zone est 1 (pour «enregistrement de type 1»). Le deuxième élément d'information est le nombre des autres enregistrements contenus dans le fichier. Ce nombre est égal au total des sous-zones restantes de la zone 1 003.

Chacune des sous-zones restantes est associée à un enregistrement du fichier, et l'ordre des sous-zones correspond à l'ordre des enregistrements. Chaque sous-zone contient deux éléments d'information. Le premier élément correspond au type de l'enregistrement. Le deuxième élément est l'IDC de l'enregistrement. Les deux éléments d'information présents dans chaque sous-zone sont séparés par le caractère «US».

3.1.4. Zone 1.004: TOT (Type of Transaction — type d'opération)

Cette zone contient un code mnémonique de trois lettres qui désigne le type d'opération. Ces codes sont différents de ceux utilisés dans d'autres versions de la norme ANSI/NIST.

CPS (Criminal Print-to-Print Search — comparaison d'empreintes dans le cadre d'une infraction) correspond à une recherche de concordance entre des empreintes relevées dans le cadre d'une infraction et celles enregistrées dans une base de données. Les empreintes de la personne doivent figurer dans le fichier sous la forme d'une image compressée au moyen de l'algorithme WSQ.

En cas de non-concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2.

En cas de concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2,

— 1-14 enregistrement(s) de type 4.

Le TOT CPS est résumé au tableau A.6.1 (annexe 6).

PMS (Print-to-Latent Search — comparaison empreintes/traces) correspond à une recherche de concordance entre un ensemble d'empreintes et les traces non identifiées enregistrées dans une base de données. La réponse comportera le résultat (concordance ou non-concordance) de la recherche effectuée par le FAED destinataire. S'il y a plusieurs traces non identifiées, plusieurs opérations SRE seront générées, chaque opération concernant une trace latente. Les empreintes de la personne doivent figurer dans le fichier sous la forme d'une image compressée au moyen de l'algorithme WSQ.

En cas de non-concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2.

En cas de concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2,

— 1 enregistrement de type 13.

Le TOT PMS est résumé au tableau A.6.1 (annexe 6).

MPS (Latent-to-Print Search — comparaison trace/empreintes) correspond à une recherche de concordance entre une trace relevée et les empreintes enregistrées dans une base de données. Les points caractéristiques et l'image correspondant à la trace (compressée au moyen de l'algorithme WSQ) doivent figurer dans le fichier.

En cas de non-concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2.

En cas de concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2,

— 1 enregistrement de type 4 ou de type 15.

Le TOT MPS est résumé au tableau A.6.4 (annexe 6).

MMS (Latent-to-Latent Search — comparaison trace/traces): le fichier contient une trace qu'il s'agit de comparer aux traces non identifiées enregistrées dans une base de données, afin d'établir s'il existe des liens entre diverses scènes de crime. Les points caractéristiques et l'image correspondant à la trace (compressée au moyen de l'algorithme WSQ) doivent figurer dans le fichier.

En cas de non-concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2.

En cas de concordance, les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2,

— 1 enregistrement de type 13.

Le TOT MMS est résumé au tableau A.6.4 (annexe 6).

SRE (Search Results — résultats de recherche): cette opération est générée par l'agence destinataire en réponse à des requêtes dactyloscopiques. La réponse comporte le résultat (concordance ou non-concordance) de la recherche effectuée par le FAED destinataire. S'il y a plusieurs candidats, plusieurs opérations SRE seront générées, chaque opération concernant un candidat.

Le TOT SRE est résumé au tableau A.6.2 (annexe 6).

ERR (erreur): cette opération est générée par le FAED destinataire pour indiquer qu'une erreur s'est produite. Elle comporte un message (ERM) indiquant l'erreur détectée. Les enregistrements logiques ci-après seront renvoyés:

— 1 enregistrement de type 1,

— 1 enregistrement de type 2.

Le TOT ERR est résumé au tableau A.6.3 (annexe 6).

Tableau 2: types d'enregistrements spécifiés dans les différents types d'opérations

Type d'opération	Type d'enregistrement logique					
	1	2	4	9	13	15
CPS	O	O	O	—	—	—
SRE	O	O	C	— (C en cas de concordance de traces)	C	C
MPS	O	O	—	O (1*)	O	—

Type d'opération	Type d'enregistrement logique					
	1	2	4	9	13	15
MMS	O	O	—	O (1*)	O	—
PMS	O	O	O*	—	—	O*
ERR	O	O	—	—	—	—

O = obligatoire

O* = un seul des deux types d'enregistrements peut être inclus

F = facultatif

C = à condition que des données soient disponibles

— = interdit

1* = Pour les systèmes anciens uniquement, à condition que des données soient disponibles

3.1.5. Zone 1.005: DAT (Date of Transaction — date d'opération)

Cette zone indique la date à laquelle l'opération a été lancée. Elle doit être au format ISO, c'est-à-dire: AAAAMMJJ

AAAA correspondant à l'année, MM au mois et JJ au jour. Les éléments à un seul chiffre doivent être complétés par des zéros à gauche. Par exemple, «19931004» signifie «4 octobre 1993».

3.1.6. Zone 1.006: PRY (Priority — priorité)

Cette zone facultative définit le niveau de priorité de la demande, qui peut varier de 1 à 9. 1 est la priorité la plus élevée et 9 la priorité la plus basse. Les opérations ayant la priorité 1 sont traitées immédiatement.

3.1.7. Zone 1.007: DAI (Destination Agency Identifier — identificateur du service destinataire)

Cette zone indique le service destinataire de la demande.

Elle comporte deux éléments d'information et se présente sous le format suivant: *CC*/*service*.

CC correspond au code de pays membre d'Interpol, composé de deux caractères alphanumériques, tel qu'il est défini par la norme ISO 3166. *Service* désigne le service destinataire, en trente-deux caractères alphanumériques au maximum.

3.1.8. Zone 1.008: ORI (Originating Agency Identifier — identificateur du service expéditeur)

Cette zone désigne l'expéditeur du fichier et se présente sous le même format que DAI (zone 1 007).

3.1.9. Zone 1.009: TCN (Transaction Control Number — référence de l'opération)

Cette référence est générée par l'ordinateur et doit se présenter sous le format suivant: AASSSSSSSSC,

AA correspondant à l'année de l'opération, SSSSSSSS à un numéro de série à huit chiffres et C à un caractère de contrôle calculé au moyen des formules exposées dans l'annexe 2.

En l'absence de TCN, la partie AASSSSSSSS est complétée par des zéros et C est calculé normalement.

3.1.10. Zone 1.010: TCR (Transaction Control Response — référence de la réponse)

Dans le cas d'une réponse à une demande, cette zone facultative contient la référence de la demande. Elle se présente donc sous le même format que TCN (zone 1 009).

3.1.11. Zone 1.011: NSR (Native Scanning Resolution — résolution de numérisation du système demandeur)

Cette zone définit la résolution normale de numérisation du système de l'auteur de la demande. La résolution est spécifiée sous la forme de deux chiffres suivis de la marque décimale et de deux autres chiffres.

Pour l'ensemble des opérations effectuées au titre de la décision 2008/615/JAI, la résolution est de 500 pixels/pouce ou 19,68 pixels/mm.

3.1.12. Zone 1.012: NTR (Nominal Transmitting Resolution — résolution de transmission)

Cette zone de cinq octets spécifie la résolution de transmission des images. Elle est exprimée en pixels/mm, sous le même format que NSR (zone 1 011).

3.1.13. Zone 1.013: DOM (Domain Name — nom de domaine)

Cette zone obligatoire indique le nom de domaine de la version utilisée pour formater l'enregistrement de type 2 (défini par l'utilisateur). Elle comprend deux éléments d'informations et se présente comme suit: «INT-I{US}4.21{GS}».

3.1.14. Zone 1.014: GMT (Greenwich Mean Time — heure de Greenwich)

Cette zone obligatoire permet de préciser la date et l'heure en temps universel. Elle s'ajoute à la date «en temps local» indiquée dans la zone 1 005 (DAT). Le fait de spécifier la zone GMT élimine les incohérences qui peuvent se produire lorsqu'une opération et sa réponse sont transmises entre deux sites séparés par plusieurs fuseaux horaires. Le temps universel permet de spécifier une date et une heure en temps universel sur 24 heures indépendamment des fuseaux horaires. Cette zone se présente sous la forme d'une chaîne de quinze caractères au format suivant: «SSAAMMJJHHMMSSZ». SSCAA représente l'année de l'opération, MM représente le mois, JJ représente le jour, HH représente l'heure, MM représente les minutes, SS représente les secondes. La date complète ne peut pas être postérieure à la date en cours.

4. ***Enregistrement logique de type 2: descriptif***

La majeure partie de l'enregistrement «descriptif» n'est pas définie par la norme ANSI/NIST. Cet enregistrement contient des informations spécifiques intéressant les services qui envoient ou reçoivent le fichier. Afin que les systèmes de reconnaissance automatique des empreintes digitales puissent communiquer entre eux sans problèmes, il est nécessaire que seules les zones décrites ci-après soient définies. Leur caractère obligatoire ou facultatif est précisé, et leur structure décrite.

4.1. *Les différentes zones de l'enregistrement logique de type 2*

4.1.1. Zone 2.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Cette zone obligatoire définit la longueur de l'enregistrement de type 2: elle indique le nombre total d'octets, en comptant tous les caractères de toutes les zones et les séparateurs.

4.1.2. Zone 2.002: IDC (Image Designation Character — caractère d'identification de l'image)

Cette zone obligatoire contient la représentation ASCII de l'IDC spécifié dans la zone CNT de l'enregistrement de type 1 (zone 1 003).

4.1.3. Zone 2.003: SYS (System Information — version d'INT-I utilisée)

Cette zone obligatoire est d'une longueur de quatre octets. Elle indique d'après quelle version d'INT-I est défini cet enregistrement de type 2.

Les deux premiers octets spécifient le numéro de version et les deux suivants le numéro de révision: par exemple, «version 4 révision 22» seraient spécifiés sous la forme 0422.

4.1.4. Zone 2.007: CNO (Case Number — numéro d'affaire)

C'est le numéro attribué par le service de dactyloscopie concerné à un ensemble de traces latentes relevées sur les lieux d'une infraction. Il doit être spécifié sous le format suivant: CC/numéro.

CC est le code de pays membre d'Interpol, en deux caractères alphanumériques. *numéro* est défini en fonction des exigences locales; il peut comporter jusqu'à trente-deux caractères alphanumériques.

Cette zone permet au système d'identifier les traces associées à une infraction donnée.

4.1.5. Zone 2.008: SQN (Sequence Number — numéro de la série de traces)

Ce numéro identifie chaque série de traces dans le cadre d'une affaire donnée. Il peut comporter jusqu'à quatre chiffres. Une série est constituée d'une trace ou d'un ensemble de traces regroupées à des fins de classement et/ou de recherche. Cette définition implique qu'il faut attribuer un numéro de série même à une seule trace.

Associée à MID (zone 2 009), cette zone peut servir à identifier une trace donnée dans une série.

4.1.6. Zone 2.009: MID (Latent Identifier — identificateur de trace)

Désigne une trace donnée dans une série au moyen d'une seule lettre: «A» désigne la première trace, «B» la deuxième, etc. jusqu'à «ZZ». Cette zone est utilisée comme SQN (zone 2 008).

4.1.7. Zone 2.010: CRN (Criminal Reference Number — numéro de référence du malfaiteur)

C'est le numéro de référence unique attribué par le service d'un pays à un individu qui est accusé pour la première fois d'avoir commis une infraction. Dans un pays donné, un individu ne peut avoir qu'un seul CRN et ce CRN ne peut pas être le même que celui d'un autre. Cependant, le même individu peut avoir des CRN différents dans différents pays (repérables par le code du pays).

La zone CRN se présente sous le format suivant: *CC/numéro*

CC est le code de pays selon la norme ISO 3166, en deux caractères alphanumériques; numéro est défini en fonction des règles en vigueur dans le pays où se trouve le service émetteur de la demande; il peut comporter jusqu'à trente-deux caractères alphanumériques.

En ce qui concerne les opérations effectuées au titre de la décision 2008/615/JAI, cette zone sera utilisée pour le numéro national de référence du malfaiteur attribué par le service expéditeur et lié aux images figurant dans les enregistrements logiques de types 4 ou 5.

4.1.8. Zone 2.012: MN1 (Miscellaneous Identification Number — numéro d'identification 1)

Cette zone contient le CRN (zone 2 010) transmis par une opération CPS ou PMS, sans le code du pays.

4.1.9. Zone 2.013: MN2 (Miscellaneous Identification Number — numéro d'identification 2)

Cette zone contient le CNO (zone 2 007) transmis par une opération MPS ou MMS, sans le code du pays.

4.1.10. Zone 2.014: MN3 (Miscellaneous Identification Number — numéro d'identification 3)

Cette zone contient le SQN (zone 2 008) transmis par une opération MPS ou MMS.

4.1.11. Zone 2.015: MN4 (Miscellaneous Identification Number — numéro d'identification 4)

Cette zone contient le MID (zone 2 009) transmis par une opération MPS ou MMS.

4.1.12. Zone 2.063: INF (Additional Information — informations complémentaires)

En cas d'opération SRE en réponse à une demande PMS, cette zone donne des informations sur le doigt ayant entraîné la concordance éventuelle. Le format de cette zone est le suivant:

NN, où *NN* est le code à deux chiffres correspondant à la position du doigt, tel qu'indiqué au tableau 5.

Dans tous les autres cas, cette zone est facultative. Elle comprend trente-deux caractères alphanumériques et peut donner des informations complémentaires sur la demande.

4.1.13. Zone 2.064: RLS (Respondents List — liste des réponses)

Cette zone contient au minimum deux sous-zones. La première indique le type de recherche qui a été effectuée, spécifié à l'aide du code de trois lettres utilisé dans TOT (zone 1 004). La deuxième sous-zone contient un seul caractère: «I» s'il y a correspondance (HIT), ou «N» si aucune correspondance n'a été trouvée (NOHIT). La troisième sous-zone contient le numéro de série de la proposition et le nombre total de propositions, ces deux éléments d'information étant séparés par une barre oblique. Il est transmis autant de messages que de propositions.

En cas de correspondance possible (HIT), la quatrième sous-zone contient une note, d'une longueur maximum de six chiffres. Si cette correspondance a été vérifiée, la sous-zone a la valeur «999999».

Exemple: «CPS{RS}I{RS}001/005{RS}10205{GS}»

Si le système FAED distant n'attribue pas de note, c'est la note «0» qui est attribuée.

4.1.14. Zone 2.074: ERM (Status/Error Message Field — message d'état/d'erreur)

Cette zone contient les messages d'erreur qui résultent des opérations; ces messages seront transmis à l'auteur de la demande dans le cadre d'une opération ERR.

Tableau 3: messages d'erreur

Code numérique (1-3)	Signification (5-128)
003	ERREUR: ACCÈS NON AUTORISÉ
101	Zone obligatoire manquante
102	Type d'enregistrement incorrect
103	Zone non définie
104	Nombre supérieur au maximum autorisé
105	Nombre de sous-zones incorrect
106	Longueur de zone insuffisante
107	Longueur de zone excessive
108	La zone doit contenir une valeur numérique
109	Valeur numérique trop faible dans la zone
110	Valeur numérique trop élevée dans la zone
111	Caractère incorrect
112	Date incorrecte
115	Valeur d'élément incorrecte
116	Type d'opération incorrect
117	Données de l'enregistrement incorrectes
201	ERREUR: TCN INCORRECT
501	ERREUR: QUALITÉ DES EMPREINTES INSUFFISANTE
502	ERREUR: EMPREINTES MANQUANTES
503	ERREUR: ÉCHEC DU CONTRÔLE DE LA SÉQUENCE D'EMPREINTES DIGITALES
999	ERREUR: AUTRE. POUR PLUS DE DÉTAILS, ADRESSEZ-VOUS AU SERVICE DESTINATAIRE

Messages d'erreur numérotés de 100 à 199:

Ces messages d'erreur concernent la conformité des enregistrements aux critères définis par la norme ANSI/NIST. Ils sont définis de la façon suivante:

<code_erreur 1>: IDC <nombre_idc 1> FIELD <id_zone 1> <texte dynamique 1> LF

<code_erreur 2>: IDC <nombre_idc 2> FIELD <id_zone 2> <texte dynamique 2>…

où:

— code_erreur est un code unique correspondant à une explication donnée (voir le tableau 3),

— id_zone est le numéro de la zone incorrecte, tel qu'il est défini dans la norme ANSI/NIST (par exemple, 1.01, 2 001, ...). Il est défini sous la forme <type_enregistrement>.<id_zone>.<id_sous-zone>,

— texte dynamique est une description dynamique plus détaillée de l'erreur,

— LF est un code d'avance ligne séparant les différentes erreurs,

— pour les enregistrements de type 1, le DCI a la valeur «-1».

Exemple:

201: IDC - 1 FIELD 1009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2003 INVALID SYSTEM INFORMATION

Cette zone est obligatoire pour les opérations ERR.

4.1.15. Zone 2.320: ENC (Expected Number of Candidates — nombre de propositions attendues)

Cette zone contient le nombre maximal de propositions attendues, à des fins de vérification, par le service demandeur. La valeur d'ENC ne doit pas être supérieure aux valeurs définies au tableau 11.

5. ***Enregistrement logique de type 4: image à haute résolution avec nuances de gris***

L'enregistrement logique de type 4 est de type binaire, et non de type ASCII. Chaque zone a donc une position spécifique dans l'enregistrement, ce qui implique que toutes les zones sont obligatoires. La norme permet de définir la taille et la résolution de l'image dans l'enregistrement même. Les images d'empreintes digitales contenues dans les enregistrements de type 4 doivent avoir une résolution de transmission de 500 à 520 pixels par pouce. Pour les nouveaux systèmes, la résolution minimale est de 500 pixels par pouce (soit 19,68 pixels par mm). INT-I prévoit une résolution de 500 pixels par pouce, ce qui n'empêche pas des systèmes semblables de communiquer entre eux à une autre résolution, dans la limite de 500 à 520 pixels par pouce.

5.1. *Les différentes zones de l'enregistrement logique de type 4*

5.1.1. Zone 4.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Zone de quatre octets définissant la longueur de l'enregistrement logique de type 4, c'est-à-dire son nombre total d'octets, en comptant chaque octet de chaque zone.

5.1.2. Zone 4.002: IDC (Image Designation Character — caractère d'identification de l'image)

Zone d'un octet contenant la représentation en binaire de l'IDC spécifié dans l'enregistrement d'en-tête.

5.1.3. Zone 4.003: IMP (Impression Type — méthode d'obtention de l'image)

Zone d'un octet constituant le sixième octet de l'enregistrement.

Tableau 4: méthodes d'obtention des images d'empreintes digitales

Code	Description
0	Numérisation directe d'empreinte à plat
1	Numérisation directe d'empreinte roulée
2	Numérisation d'empreinte à plat à partir d'un support papier
3	Numérisation d'empreinte roulée à partir d'un support papier
4	Photographie numérique de trace latente
5	Reproduction manuelle agrandie de trace latente

Code	Description
6	Photo argentique de trace latente
7	Transfert de trace latente
8	Relevé à l'aide d'un lecteur magnétique
9	Inconnu

5.1.4. Zone 4.004: FGP [(Finger Position — doigt(s) concerné(s)]

Zone d'une longueur fixe de six octets occupant les octets 7 à 12 de l'enregistrement de type 4. Elle désigne les doigts concernés, en commençant par l'octet de gauche (le septième). La position connue ou la plus probable du doigt est reprise du tableau 5. On peut spécifier jusqu'à cinq doigts supplémentaires dans les cinq octets restants, de la même façon. Si l'on spécifie moins de cinq doigts, on spécifie l'équivalent binaire de 255 dans les octets non utilisés. Lorsqu'on ne sait pas de quel doigt il s'agit, on spécifie le code 0.

Tableau 5: codes des différents doigts et dimensions de l'image

Doigt	Code	Largeur maximale (mm)	Longueur maximale (mm)
Doigt non identifié	0	40,0	40,0
Pouce droit	1	45,0	40,0
Index droit	2	40,0	40,0
Majeur droit	3	40,0	40,0
Annulaire droit	4	40,0	40,0
Auriculaire droit	5	33,0	40,0
Pouce gauche	6	45,0	40,0
Index gauche	7	40,0	40,0
Majeur gauche	8	40,0	40,0
Annulaire gauche	9	40,0	40,0
Auriculaire gauche	10	33,0	40,0
Empreinte à plat du pouce droit	11	30,0	55,0
Empreinte à plat du pouce gauche	12	30,0	55,0
Empreintes à plat des quatre autres doigts de la main droite	13	70,0	65,0
Empreintes à plat des quatre autres doigts de la main gauche	14	70,0	65,0

Pour les traces latentes, seules les valeurs 0 à 10 peuvent être utilisées.

5.1.5. Zone 4.005: ISR (Image Scanning Resolution — résolution de numérisation)

Zone d'un octet constituant le treizième octet de l'enregistrement de type 4. Elle contient 0 si l'image a été scannée à la résolution de 19,68 pixels/mm (500 pixels par pouce). Elle contient 1 si l'image a été scannée à une autre résolution (information spécifiée dans l'enregistrement d'en-tête).

5.1.6. Zone 4.006: HLL (Horizontal Line Length — longueur de ligne)

Cette zone occupe les octets 14 et 15 de l'enregistrement de type 4. Elle spécifie le nombre de pixels de chaque ligne de numérisation. Le premier octet est le plus significatif.

5.1.7. Zone 4.007: VLL (Vertical Line Length – longueur de colonne)

Cette zone occupe les octets 16 et 17 de l'enregistrement de type 4. Elle spécifie le nombre de colonnes de numérisation de l'image. Le premier octet est le plus significatif.

5.1.8. Zone 4.008: GCA (Gray-scale Compression Algorithm — algorithme de compression de l'échelle de gris)

Zone d'un octet spécifiant l'algorithme de compression de l'échelle de gris utilisé pour l'image. Pour la mise en œuvre en question, le code binaire 1 signifie que l'algorithme de compression WSQ (annexe 7) a été utilisé.

5.1.9. Zone 4.009: Image (image)

Cette zone contient une suite d'octets représentant l'image. Sa structure dépend évidemment de l'algorithme de compression utilisé.

6. ***Enregistrement logique de type 9: points caractéristiques***

L'enregistrement logique de type 9 contient du texte ASCII décrivant les points caractéristiques (ou minuties) d'une trace latente et les informations qui s'y rapportent. En ce qui concerne les opérations de recherche de trace latente, les enregistrements de type 9 ne sont pas limités en nombre dans un fichier, chaque enregistrement correspondant à une vue différente ou à une trace latente différente.

6.1. *Extraction des points caractéristiques*

6.1.1. Identification du type de points caractéristiques

La présente norme définit trois numéros d'identification désignant les différents types de points caractéristiques. Le tableau 6 résume la signification de ces numéros d'identification. Le type 1 correspond à un arrêt de ligne. Le type 2 correspond à une bifurcation. Lorsqu'un point caractéristique ne relève pas clairement de l'une des deux catégories ci-dessus mentionnées, il est dit «autre», ce qui correspond au type 0.

Tableau 6: types de points caractéristiques

Type	Description
0	Autre
1	Arrêt de ligne
2	Bifurcation

6.1.2. Type et emplacement des points caractéristiques

Afin de mettre les modèles en conformité avec la section 5 de la norme ANSI INCITS 378-2004, on aura recours à la méthode décrite ci-dessous, qui améliore la norme INCITS 378-2004 actuelle, pour déterminer l'emplacement (localisation et direction angulaire) de chaque point caractéristique.

Le positionnement ou la localisation d'un point caractéristique représentant un arrêt (ou terminaison) de ligne (ou crête) est le point situé juste avant l'arrêt de ligne, à l'endroit où la partie commune de la vallée (creux) se sépare en deux branches. Si les trois branches de la vallée (creux) sont réduites à un squelette d'une largeur de 1 pixel, le point caractéristique est le point d'intersection. À l'inverse, la localisation d'un point caractéristique représentant une bifurcation est le point où la partie commune de la crête se sépare en deux branches. Si les trois branches de la crête sont réduites à un squelette d'une largeur de 1 pixel, le point caractéristique est le point d'intersection.

Après conversion de toutes les terminaisons en bifurcations, tous les points caractéristiques de l'image dactyloscopique sont représentés par des bifurcations. Les coordonnées X et Y, exprimées en pixels, de l'intersection des trois branches de chaque point caractéristique, peuvent être formatées directement. À partir de chaque bifurcation des squelettes, il est possible de déterminer la direction des points caractéristiques. Les trois branches de chaque bifurcation doivent être examinées et les terminaisons de chaque branche doivent être déterminées. La figure 6.1.2 illustre les trois méthodes mises en œuvre pour déterminer l'emplacement de la fin d'une branche sur la base d'une résolution de numérisation de 500 ppp.

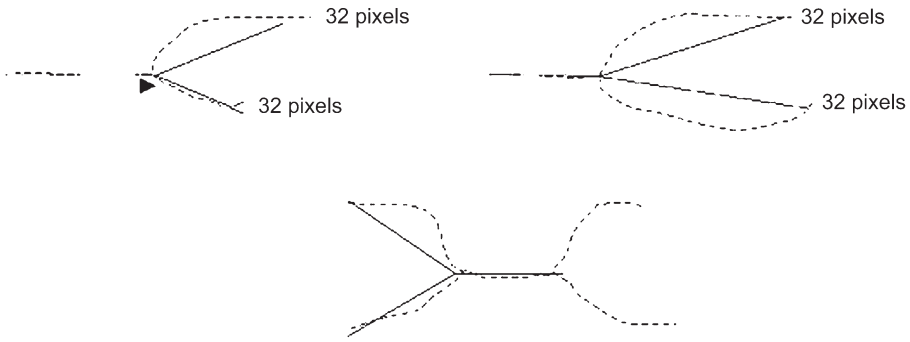
L'emplacement de la terminaison est établi en fonction de l'événement qui se produit en premier. Le comptage des pixels repose sur une numérisation à la résolution de 500 ppp. Des résolutions de numérisation différentes donneraient des comptages de pixels différents.

— Distance de 0,064 pouce (32^{e} pixel).

— La fin de la branche du squelette qui apparaît à une distance comprise entre 0,02 pouce et 0,064 pouce (entre le 10^{e} et le 32^{e} pixel): les branches les plus courtes ne sont pas utilisées.

— Une deuxième bifurcation apparaît à une distance de moins de 0,064 pouce (avant le 32^{e} pixel).

Figure 6.1.2



L'angle du point caractéristique est déterminé en construisant trois rayons virtuels ayant leur origine au point de bifurcation et s'étendant jusqu'à la fin de chaque branche. Le plus petit des trois angles formé par les rayons est divisé en deux parties égales afin d'indiquer la direction du point caractéristique.

6.1.3. Coordonnées

Les points caractéristiques d'une empreinte digitale sont décrits par un système de coordonnées cartésien. Les coordonnées X et Y des points caractéristiques représentent leur emplacement. L'origine du système de coordonnées est le coin supérieur gauche de l'image originale, X augmentant vers la droite et Y augmentant vers le bas. Les coordonnées X et Y d'un point caractéristique sont représentées en unités de pixels à partir de l'origine. Il y a lieu de noter que l'emplacement de l'origine et les unités de mesure ne sont pas conformes à la convention utilisée dans les définitions du type 9 prévues dans la norme ANSI/NIST-ITL 1-2000.

6.1.4. Direction des points caractéristiques

Les angles sont exprimés selon le format mathématique standard, le degré 0 étant placé à droite et les angles augmentant dans le sens contraire des aiguilles d'une montre. Dans le cas d'un arrêt de ligne, la direction de l'angle est en sens contraire, le long de la ligne; dans le cas d'une bifurcation, la direction de l'angle est vers le centre de la vallée. Cette convention est l'inverse de celle qui est décrite dans les définitions du type 9 dans la norme ANSI/NIST-ITL 1-2000.

6.2. *Les différentes zones de l'enregistrement logique de type 9 au format INCITS-378*

Toutes les zones de l'enregistrement de type 9 sont enregistrées sous forme de texte ASCII. Aucune valeur binaire n'est autorisée dans ce type d'enregistrement à zones balisées.

6.2.1. Zone 9.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Cette zone ASCII obligatoire définit la longueur de l'enregistrement logique, c'est-à-dire son nombre total d'octets, en comptant chaque octet de chaque zone.

6.2.2. Zone 9.002: IDC (Image Designation Character — caractère d'identification de l'image)

Cette zone obligatoire de deux octets sert à identifier et à définir l'emplacement des points caractéristiques. L'IDC contenu dans cette zone correspond à celui spécifié dans la zone CNT de l'enregistrement de type 1.

6.2.3. Zone 9.003: IMP (Impression Type — méthode d'obtention de l'image)

Cette zone obligatoire d'un octet décrit la manière dont l'image d'empreinte digitale a été obtenue. Elle contient la valeur ASCII du code approprié (voir tableau 4).

6.2.4. Zone 9.004: FMT (Minutiæ Format — présentation des points caractéristiques)

La mention «U» indique que les points caractéristiques sont présentés selon la norme M1-378. Même si les informations peuvent être encodées conformément à ladite norme M1-378, les zones des enregistrements de type 9 données doivent rester des zones de données ASCII.

6.2.5. Zone 9.126: Informations CBEFF (Common Biometric Exchange File Format — format commun d'échange de fichiers biométriques)

Cette zone comprend trois informations. La première est la valeur «27» (0x1B). Il s'agit de l'identification du possesseur CBEFF que l'International Biometric Industry Association (Association internationale de l'industrie biométrique) a attribué au comité technique M1 de l'INCITS (InterNational Committee for Information Technology Standards — Comité international pour les normes informatiques). Le caractère <US> délimite cette information du type de format CBEFF, auquel la valeur «513» (0x0201) est attribuée, pour indiquer que

l'enregistrement concerné ne contient que des données relatives à l'emplacement et à la direction angulaire, en l'absence de toute information de type bloc de données. Le caractère <US> délimite cette information de l'identifiant de produit (PID) CBEFF, qui désigne le «possesseur» du matériel d'encodage. C'est le vendeur qui établit cette valeur. Elle peut être obtenue sur le site web de l'IBIA (www.ibia.org), si elle a été publiée.

6.2.6. Zone 9.127: identification du matériel de numérisation

Cette zone contient deux informations séparées par le caractère <US>. La première est «APPF» si le matériel utilisé à l'origine pour numériser l'image est certifié conforme à l'appendice F de la norme CJIS-RS-0010 (spécifications concernant la qualité de l'image dans le cadre de l'Integrated Automated Fingerprint Identification System — IAFIS — système intégré et automatisé d'identification des empreintes digitales), c'est-à-dire les spécifications établies par le Federal Bureau of Investigations des États-Unis (FBI) concernant la transmission des empreintes digitales par voie électronique. Si le matériel n'est pas conforme, cette zone comprend la mention «NONE». La deuxième information comprend l'identifiant du matériel de numérisation, c'est-à-dire un numéro attribué par le distributeur du produit. La valeur «0» signifie que l'identifiant du matériel de numérisation est inconnu.

6.2.7. Zone 9.128: HLL (Horizontal Line Length — longueur de ligne)

Cette zone ASCII obligatoire indique le nombre de pixels d'une ligne de l'image transmise. La taille horizontale maximale est de 65 534 pixels.

6.2.8. Zone 9.129: VLL (Vertical Line Length — longueur de colonne)

Cette zone ASCII obligatoire indique le nombre de lignes de l'image transmise. La taille verticale maximale est de 65 534 pixels.

6.2.9. Zone 9.130: SLC (Scale Units — unités de résolution utilisées)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels de l'image. 1 indique que l'on s'exprime en «pixels par pouce», et 2 que l'on s'exprime en «pixels par centimètre». 0 indique qu'aucune unité n'est précisée. Dans ce cas, c'est le quotient de HPS/VPS qui donne le rapport largeur/hauteur.

6.2.10. Zone 9.131: HPS (Horizontal Pixel Scale — unité utilisée pour les lignes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels entiers des lignes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante horizontale du rapport largeur/hauteur.

6.2.11. Zone 9.132: VPS (Vertical Pixel Scale — unité utilisée pour les colonnes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels entiers des colonnes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante horizontale du rapport largeur/hauteur.

6.2.12. Zone 9.133: vue de l'empreinte digitale

Dans cette zone obligatoire figure le numéro de vue correspondant à l'empreinte digitale associée aux données présentes dans l'enregistrement concerné. Le numéro de vue va de «0» à «15» par sauts de 1.

6.2.13. Zone 9.134: FGP [(Finger Position — doigt(s) concerné(s)]

Dans cette zone obligatoire figure le code correspondant à la position du doigt à l'origine des informations présentes dans cet enregistrement de type 9. Un code compris entre 1 et 10, tiré du tableau 5, ou le code correspondant aux différentes parties de l'empreinte palmaire, tiré du tableau 10, sera utilisé pour désigner la position de l'empreinte digitale ou palmaire.

6.2.14. Zone 9.135: qualité de l'empreinte digitale

Cette zone indique, par un code compris entre 0 et 100, la qualité d'ensemble des données correspondant aux points caractéristiques des empreintes concernées. Ce nombre exprime la qualité globale de l'enregistrement correspondant aux empreintes et représente la qualité de l'image originale, de l'extraction des points caractéristiques et de toute opération complémentaire susceptible d'influencer l'enregistrement des points caractéristiques.

6.2.15. Zone 9.136: décompte des points caractéristiques

Cette zone obligatoire indique le nombre de points caractéristiques enregistrés dans l'enregistrement logique concerné.

6.2.16. Zone 9.137: données relatives aux points caractéristiques

Cette zone obligatoire comprend six informations séparées par le caractère <US>. Elle comprend plusieurs sous-zones, chacune comprenant les données relatives à un point caractéristique. Le nombre de sous-zones doit être le même que le nombre indiqué dans la zone 136. La première information est le numéro d'index du point caractéristique: la première a le numéro «1», ce chiffre étant augmenté par saut de 1 pour les points caractéristiques suivants. Les deuxième et troisième informations sont, respectivement, les coordonnées X et Y du point caractéristique, exprimées en pixels. La quatrième information est l'angle du point caractéristique, enregistré par unités de deux degrés. Il s'agit d'une valeur non négative comprise entre 0 et 179. La cinquième information est le type de point caractéristique. La valeur «0» représente un point caractéristique de type «OTHER» (autre), la valeur «1» une terminaison et la valeur «2» une bifurcation. La sixième information porte sur la qualité de chaque point caractéristique. Sa valeur va de 1 au minimum à 100 au maximum. La valeur «0» indique qu'aucune information n'est disponible sur la qualité. Chaque sous-zone est séparée de la suite par le caractère <US>.

6.2.17. Zone 9.138: décompte de crêtes

Cette zone comprend une série de sous-zones, chacune contenant trois informations. La première information de la première sous-zone indique la méthode utilisée pour dénombrer les crêtes. La valeur «0» indique qu'aucune hypothèse ne peut être émise sur la méthode utilisée pour extraire l'information relative au décompte des crêtes ou à leur ordre dans l'enregistrement. La valeur «1» indique que, pour chaque point caractéristique central, les données relatives au décompte des crêtes ont été extraites par rapport aux points caractéristiques les plus proches, en quatre quadrants, et que les nombres de crêtes pour chaque point caractéristique central sont présentés ensemble. La valeur «2» indique que, pour chaque point caractéristique central, les données relatives au décompte des crêtes ont été extraites par rapport aux points caractéristiques les plus proches, en huit quadrants, et que les nombres de crêtes pour chaque point caractéristique central sont présentés ensemble. Les deux informations restantes de la première sous-zone contiennent toutes les deux la valeur «0». Les informations sont séparées les unes des autres par le caractère <US>. Les sous-zones suivantes contiennent trois informations: la première est le numéro d'index du point caractéristique central, la deuxième est le numéro d'index des points caractéristiques voisins et la troisième est le nombre de crêtes traversées. Les sous-zones sont séparées les unes des autres par le caractère <RS>.

6.2.18. Zone 9.139: informations sur le centre de figure

Cette zone comprend une sous-zone pour chaque centre de figure présent dans l'image originale. Chaque sous-zone contient trois informations: les deux premières sont les coordonnées X et Y en pixels. La troisième est l'angle du centre de figure, enregistré par unités de deux degrés. Il s'agit d'une valeur non négative comprise entre 0 et 179. Les différents centres de figure seront séparés par le caractère <RS>.

6.2.19. Zone 9.140: informations sur les deltas

Cette zone comprend une sous-zone pour chaque delta présent dans l'image originale. Chaque sous-zone contient trois informations: les deux premières sont les coordonnées X et Y en pixels. La troisième est l'angle du delta, enregistré par unités de deux degrés. Il s'agit d'une valeur non négative comprise entre 0 et 179. Les différents deltas seront séparés par le caractère <RS>.

7. ***Enregistrement logique de type 13: image de trace latente à résolution variable***

L'enregistrement logique de type 13 à zones balisées contient des données concernant des images latentes. Ces images doivent être transmises à des services qui procéderont eux-mêmes à l'extraction (automatique ou manuelle) des informations voulues.

Les informations relatives à la résolution utilisée pour la numérisation et à la taille de l'image, ainsi que les autres paramètres nécessaires au traitement de l'image sont enregistrés en tant que zones balisées au sein de l'enregistrement.

Tableau 7 — récapitulatif des différentes zones de l'enregistrement logique de type 13

Nom de la zone	Statut	Numéro de la zone	Nom complet de la zone	Type de caractère	Taille pour chaque occurrence de la zone		Nombre d'occurrences autorisé		Nombre maximal d'octets
					minimale	maximale	minimal	maximal	
LEN	M	13.001	LOGICAL RECORD LENGTH (LONGUEUR DE L'ENREGISTREMENT LOGIQUE)	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER (CARACTÈRE D'IDENTIFICATION DE L'IMAGE)	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE (MÉTHODE D'OBTENTION DE L'IMAGE)	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY/ORI (SERVICE D'ORIGINE)	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE DATE (DATE D'ACQUISITION DE L'IMAGE LATENTE)	N	9	9	1	1	16

Nom de la zone	Statut	Numéro de la zone	Nom complet de la zone	Type de caractère	Taille pour chaque occurrence de la zone		Nombre d'occurrences autorisé		Nombre maximal d'octets
					minimale	maximale	minimal	maximal	
HLL	M	13.006	HORIZONTAL LINE LENGTH (LONGUEUR DE LIGNE)	N	4	5	1	1	12
VLL	M	13.007	VERTICAL LINE LENGTH (LONGUEUR DE COLONNE)	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS (UNITÉS DE RÉSOLUTION UTILISÉES)	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE (UNITÉ UTILISÉE POUR LES LIGNES)	N	2	5	1	1	12
VPS	O	13.010	VERTICAL PIXEL SCALE (UNITÉ UTILISÉE POUR LES COLONNES)	N	2	5	1	1	12
CGA	O	13.011	COMPRESSION ALGORITHM (ALGORITHME DE COMPRESSION)	A	5	7	1	1	14
BPX	O	13.012	BITS PER PIXEL (NOMBRE DE BITS PAR PIXEL)	N	2	3	1	1	10
FGP	O	13.013	FINGER POSITION (DOIGT(S) CONCERNÉ(S)]	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION (RESERVÉES EN VUE D'UNE DÉFINITION ULTÉRIEURE)	—	—	—	—	—	—
COM	F	13.020	COMMENT (COMMENTAIRE)	A	2	128	0	1	135
RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION (RESERVÉES EN VUE D'UNE DÉFINITION ULTÉRIEURE)	—	—	—	—	—	—
UDF	F	13.200 13.998	USER-DEFINED FIELDS (ZONES DÉFINIES PAR L'UTILISATEUR)	—	—	—	—	—	—
DAT	O	13.999	IMAGE DATA (DONNÉES CONCERNANT L'IMAGE)	B	2	—	1	1	—

O = obligatoire F = facultatif

Type de caractères: N = numérique A = alphabétique AN = alphanumérique B = binaire

7.1. *Les différentes zones de l'enregistrement logique de type 13*

Les paragraphes qui suivent décrivent le contenu de chacune des zones de l'enregistrement logique de type 13.

Dans ce type d'enregistrements, les données doivent être spécifiées dans des zones numérotées. Les deux premières zones de l'enregistrement doivent se présenter toujours dans le même ordre, et la zone contenant les données relatives à l'image doit être la dernière de l'enregistrement. Le tableau 7 indique, pour chaque zone de l'enregistrement de type 13, le caractère obligatoire ou facultatif de celle-ci, son numéro, son nom, le type de caractères qu'elle contient, sa dimension en nombre de caractères et ses conditions d'occurrence. La dernière colonne du tableau précise la taille maximale de chaque zone, en nombre d'octets. Si l'on utilise plus de trois chiffres pour le numéro de zone, la taille maximale augmente. Les nombres précisés dans les deux sous-colonnes de «taille pour chaque occurrence de la zone» prennent en compte tous les séparateurs utilisés au sein de la zone concernée. Le nombre maximal d'octets indiqué englobe le numéro de la zone, les informations et tous les séparateurs, y compris le caractère «GS».

7.1.1. Zone 13.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Cette zone ASCII obligatoire définit le nombre d'octets total de l'enregistrement, en comptant chaque caractère de chaque zone et les séparateurs.

7.1.2. Zone 13.002: IDC (Image Designation Character — caractère d'identification de l'image)

Cette zone ASCII obligatoire sert à identifier l'image latente contenue dans l'enregistrement. L'IDC qu'elle contient doit être le même que celui contenu dans la zone CNT de l'enregistrement de type 1.

7.1.3. Zone 13.003: IMP (Impression Type — méthode d'obtention de l'image)

Cette zone obligatoire d'un ou de deux octets décrit la manière dont l'image latente a été obtenue. Elle contient l'un des codes figurant dans le tableau 4 (empreinte digitale) ou 9 (empreinte palmaire).

7.1.4. Zone 13.004: ORI (SRC) (Source Agency — service d'origine)

Cette zone ASCII obligatoire donne l'identificateur du service ou de l'organisation qui a obtenu l'image latente contenue dans l'enregistrement. C'est normalement le code ORI du service ayant acquis l'image qui est contenu dans cette zone. Elle comporte deux éléments d'information et se présente sous le format suivant: CC/*service*.

CC correspond au code de pays membre d'Interpol, composé de deux caractères alphanumériques. «*Service*» désigne le service destinataire, en trente-deux caractères alphanumériques de texte libre au maximum.

7.1.5. Zone 13.005: LCD (Latent Capture Date — date d'acquisition de l'image latente)

Cette zone ASCII obligatoire contient la date à laquelle l'image contenue dans l'enregistrement a été obtenue. Elle est exprimée en huit chiffres sous le format suivant: AAAAMMJJ. AAAA correspond à l'année d'acquisition de l'image. MM correspond au mois. JJ correspond au jour. Par exemple, 20000229 correspond au 29 février 2000. La date complète doit être une date réelle.

7.1.6. Zone 13.006: HLL (Horizontal Line Length — longueur de ligne)

Cette zone ASCII obligatoire indique le nombre de pixels d'une ligne de l'image transmise.

7.1.7. Zone 13.007: VLL (Vertical Line Length — longueur de colonne)

Cette zone ASCII obligatoire indique le nombre de lignes horizontales de l'image transmise.

7.1.8. Zone 13.008: SLC (Scale Units — unités de résolution utilisées)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels de l'image. 1 indique que l'on s'exprime en «pixels par pouce», et 2 que l'on s'exprime en «pixels par centimètre». 0 indique qu'aucune unité n'est précisée. Dans ce cas, c'est le quotient de HPS/VPS qui donne le rapport largeur/hauteur.

7.1.9. Zone 13.009: HPS (Horizontal Pixel Scale — unité utilisée pour les lignes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels des lignes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante horizontale du rapport largeur/hauteur.

7.1.10. Zone 13.010: VPS (Vertical Pixel Scale — unité utilisée pour les colonnes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels des colonnes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante verticale du rapport largeur/hauteur.

7.1.11. Zone 13.011: CGA (Compression Algorithm — algorithme de compression)

Cette zone ASCII obligatoire indique l'algorithme utilisé pour compresser les images à niveaux de gris. Voir l'annexe 7 pour les codes de compression.

7.1.12. Zone 13.012: BPX (Bits Per Pixel — nombre de bits par pixel)

Cette zone ASCII spécifie le nombre de bits utilisés pour représenter un pixel. Il convient d'y spécifier «8» pour les valeurs de niveaux de gris normales comprises entre 0 et 255. Toute valeur supérieure à 8 représente un pixel en niveaux de gris de plus grande précision.

7.1.13. Zone 13.013: FGP [(Finger/Palm Position — doigt(s) concerné(s)/partie(s) de la paume concernée(s)]

Cette zone balisée obligatoire spécifie le ou les doigts, ou encore la ou les parties de paumes, pouvant correspondre à l'image latente. Elle contient l'un des codes décimaux du tableau 5 correspondant de façon certaine ou la plus probable au doigt concerné, ou l'un de ceux du tableau 10 correspondant à la partie de paume la plus probablement concernée, et se présente sous la forme d'une zone ASCII à un ou à deux caractères. D'autres codes de doigts/parties de paumes peuvent être introduits, sous forme de sous-zones séparées par le séparateur «RS». Le code «0», correspondant à «doigt non identifié», peut être utilisé pour n'importe quel doigt. Le code «20», correspondant à «image palmaire non identifiée», peut lui aussi être utilisé pour n'importe quelle partie de paume.

7.1.14. Zones 13.014 à 019: RSV (Reserved for Future Definition — réservées en vue d'une définition ultérieure)

Les zones concernées seront définies dans les futures révisions de la présente norme. Aucune d'entre elles ne doit être utilisée dans le cadre de la présente révision. Si l'une d'elles est spécifiée, elle ne doit pas être prise en compte.

7.1.15. Zone 13.020: COM (Comment — commentaire)

Cette zone facultative peut être utilisée pour ajouter des commentaires ou du texte ASCII aux données concernant l'image latente.

7.1.16. Zones 13.021 à 199: RSV (Reserved for Future Definition — réservées en vue d'une définition ultérieure)

Les zones concernées seront définies dans les futures révisions de la présente norme. Aucune d'entre elles ne doit être utilisée dans le cadre de la présente révision. Si l'une d'elles est spécifiée, elle ne doit pas être prise en compte.

7.1.17. Zones 13.200 à 998: UDF (User-Defined Fields — zones définies par l'utilisateur)

Ces zones peuvent être définies par l'utilisateur et seront utilisées en fonction des nécessités ultérieures. Leur taille et leur contenu sont fixés par l'utilisateur, en accord avec le service destinataire. Si elles sont spécifiées, elles contiennent du texte ASCII.

7.1.18. Zone 13.999: DAT (Image Data — données concernant l'image)

Cette zone contient toutes les indications relatives à une image latente acquise. Il convient de toujours lui attribuer le numéro 999. Elle doit toujours être la dernière zone de l'enregistrement. Par exemple, «13.999:» est suivi de données binaires sur l'image.

Chaque pixel des données d'une image à niveaux de gris non compressée est normalement décrit sur les huit bits (256 niveaux de gris) d'un seul octet. Si la zone 13.012 (BPX) contient une valeur inférieure ou supérieure à 8, le nombre d'octets requis pour décrire un pixel sera différent. Si l'image est compressée, les données relatives aux pixels seront compressées au moyen de la technique spécifiée dans la zone CGA.

7.2. *Fin de l'enregistrement logique de type 13*

Pour des raisons de cohérence, le dernier octet de la zone 13.999 doit être séparé de l'enregistrement logique suivant par le séparateur FS. Ce séparateur doit être pris en compte dans la zone LEN de l'enregistrement de type 13.

8. ***Enregistrement logique de type 15: images d'empreintes palmaires à résolution variable***

L'enregistrement logique de type 15 à zones balisées contient des données relatives aux images d'empreintes palmaires, ainsi que des zones de texte prédéfini ou défini par l'utilisateur relatives à l'image numérisée, et permet d'échanger ces données. Les informations relatives à la résolution utilisée pour la numérisation aux dimensions de l'image et aux autres paramètres ou commentaires nécessaires au traitement de l'image sont enregistrées sous forme de zones balisées au sein de l'enregistrement. Les images d'empreintes palmaires transmises aux autres services sont traitées par les destinataires qui en extraient les informations voulues aux fins de recherche de correspondances.

Les images sont obtenues soit par numérisation directe, soit à partir d'une fiche ou de tout autre support contenant les empreintes palmaires du sujet.

Toute méthode d'acquisition utilisée doit permettre d'obtenir une série d'images pour chaque main. Cette série d'images doit inclure la paume proprement dite (une seule image numérique) et la main tout entière, du poignet au bout des doigts (une ou deux images numériques). Si la totalité de la main figure sur deux images, l'image correspondant à la partie inférieure doit couvrir la partie de la main allant du poignet jusqu'en haut de la zone interdigitale/région palmaire (articulation du majeur), et doit inclure le thénar et l'hypothénar. L'image correspondant à la partie supérieure doit aller du bas de la zone interdigitale jusqu'au bout des doigts. Grâce à cette méthode, on obtient un chevauchement suffisant entre les deux images situées au niveau de la zone interdigitale/région palmaire. En rapprochant les lignes contenues dans cette zone commune, un spécialiste peut assurer avec certitude que les deux images correspondent à la même paume.

Une opération concernant une empreinte palmaire pouvant servir à différentes fins, elle peut porter sur une ou plusieurs images provenant de la paume ou de la main. Pour un individu donné, un relevé complet comprend l'empreinte palmaire proprement dite plus l'empreinte de la main complète (en une ou en deux images), et cela pour chacune des deux mains. Un enregistrement logique à zones balisées ne pouvant contenir qu'une seule zone binaire, un enregistrement de type 15 sera nécessaire pour chaque empreinte palmaire, plus un ou deux enregistrements pour chaque empreinte palmaire complète. Autrement dit, quatre à six enregistrements de type 15 seront nécessaires pour représenter les empreintes palmaires d'un sujet dans le cadre d'une opération normale.

8.1. *Les différentes zones de l'enregistrement logique de type 15*

Les paragraphes qui suivent décrivent le contenu de chacune des zones de l'enregistrement logique de type 15.

Dans ce type d'enregistrements, les données doivent être spécifiées dans des zones numérotées. Les deux premières zones de l'enregistrement doivent se présenter toujours dans le même ordre, et la zone contenant les données relatives à l'image doit être la dernière de l'enregistrement. Le tableau 8 ci-après indique, pour chaque zone de l'enregistrement de type 15, le caractère obligatoire ou facultatif de celle-ci, son numéro, son nom, le type de caractères qu'elle contient, sa dimension et ses conditions d'occurrence. La dernière colonne du tableau précise la taille maximale de chaque zone, en nombre d'octets. Si l'on utilise plus de trois chiffres pour le numéro de zone, la taille maximale augmente. Les nombres précisés dans les deux sous-colonnes de «taille pour chaque occurrence de la zone» prennent en compte tous les séparateurs utilisés au sein de la zone concernée. Le nombre maximal d'octets indiqué englobe le numéro de la zone, les informations et tous les séparateurs, y compris le caractère «GS».

8.1.1. Zone 15.001: LEN (Logical Record Length — longueur de l'enregistrement logique)

Cette zone ASCII obligatoire définit le nombre d'octets total de l'enregistrement, en comptant chaque caractère de chaque zone et les séparateurs.

8.1.2. Zone 15.002: IDC (Image Designation Character — caractère d'identification de l'image)

Cette zone ASCII obligatoire sert à identifier l'image d'empreinte palmaire contenue dans l'enregistrement. L'IDC qu'elle contient doit être le même que celui contenu dans la zone CNT de l'enregistrement de type 1.

8.1.3. Zone 15.003: IMP (Impression Type — méthode d'obtention de l'image)

Cette zone obligatoire ASCII d'un octet décrit la manière dont l'image d'empreinte palmaire a été obtenue. Elle contient l'un des codes figurant dans le tableau 9 ci-après.

8.1.4. Zone 15.004: ORI (SRC) (Source Agency — service d'origine)

Cette zone ASCII obligatoire donne l'identificateur du service ou de l'organisation qui a acquis l'image d'empreinte palmaire contenue dans l'enregistrement. C'est normalement le code ORI du service ayant acquis l'image qui est contenu dans cette zone. SRC comporte deux éléments d'information et se présente sous le format suivant: CC/*service*.

CC correspond au code de pays membre d'Interpol, composé de deux caractères alphanumériques. «*Service*» désigne le service destinataire, en trente-deux caractères alphanumériques de texte libre au maximum.

8.1.5. Zone 15.005: PCD (Palmprint Capture Date — date d'acquisition de l'image d'empreinte palmaire)

Cette zone ASCII obligatoire contient la date à laquelle l'image contenue dans l'enregistrement a été acquise. Elle est exprimée en huit chiffres sous le format suivant: AAAAMMJJ. AAAA correspond à l'année d'acquisition de l'image. MM correspond au mois. JJ correspond au jour. Par exemple, 20000229 correspond au 29 février 2000. La date complète doit être une date réelle.

8.1.6. Zone 15.006: HLL (Horizontal Line Length — longueur de ligne)

Cette zone ASCII obligatoire indique le nombre de pixels d'une ligne de l'image transmise.

8.1.7. Zone 15.007: VLL (Vertical Line Length — longueur de colonne)

Cette zone ASCII obligatoire indique le nombre de lignes horizontales de l'image transmise.

8.1.8. Zone 15.008: SLC (Scale Units — unités de résolution utilisées)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels de l'image. 1 indique que l'on s'exprime en «pixels par pouce», et 2 que l'on s'exprime en «pixels par centimètre». 0 indique qu'aucune unité n'est précisée. Dans ce cas, c'est le quotient de HPS/VPS qui donne le rapport largeur/hauteur.

8.1.9. Zone 15.009: HPS (Horizontal Pixel Scale — unité utilisée pour les lignes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels des lignes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante horizontale du rapport largeur/hauteur.

8.1.10. Zone 15.010: VPS (Vertical Pixel Scale — unité utilisée pour les colonnes)

Cette zone ASCII obligatoire indique par rapport à quelle unité de longueur est exprimée la densité en pixels des colonnes de l'image, à condition que 1 ou 2 soit spécifié dans la zone SLC. Si tel n'est pas le cas, HPS indique la composante verticale du rapport largeur/hauteur.

Tableau 8: récapitulatif des différentes zones de l'enregistrement logique de type 15

Nom de la zone	Statut	Numéro de la zone	Nom complet de la zone	Type de caractères	Taille pour chaque occurrence de la zone		Nombre d'occurrences autorisé		Nombre maximal d'octets
					minimale	maximale	minimal	maximal	
LEN	O	15.001	LOGICAL RECORD LENGTH (LONGUEUR DE L'ENREGISTREMENT LOGIQUE)	N	4	8	1	1	15
IDC	O	15.002	IMAGE DESIGNATION CHARACTER (NOMBRE DE CARACTÈRES DU FICHIER)	N	2	5	1	1	12
IMP	O	15.003	IMPRESSION TYPE (MÉTHODE D'OBTENTION DE L'IMAGE)	N	2	2	1	1	9
SRC	O	15.004	SOURCE AGENCY/ORI (SERVICE D'ORIGINE)	AN	6	35	1	1	42
PCD	O	15.005	PALMPRINT CAPTURE DATE (DATE D'ACQUISITION DE L'IMAGE D'EMPREINTE PALMAIRE)	N	9	9	1	1	16
HLL	O	15.006	HORIZONTAL LINE LENGTH (LONGUEUR DE LIGNE)	N	4	5	1	1	12
VLL	O	15.007	VERTICAL LINE LENGTH (LONGUEUR DE COLONNE)	N	4	5	1	1	12
SLC	O	15.008	SCALE UNITS (UNITÉS DE RÉSOLUTION UTILISÉES)	N	2	2	1	1	9
HPS	O	15.009	HORIZONTAL PIXEL SCALE (UNITÉ UTILISÉE POUR LES LIGNES)	N	2	5	1	1	12
VPS	O	15.010	VERTICAL PIXEL SCALE (UNITÉ UTILISÉE POUR LES COLONNES)	N	2	5	1	1	12
CGA	O	15.011	COMPRESSION ALGORITHM (ALGORITHME DE COMPRESSION)	AN	5	7	1	1	14
BPX	O	15.012	BITS PER PIXEL (NOMBRE DE BITS PAR PIXEL)	N	2	3	1	1	10
PLP	O	15.013	PALMPRINT POSITION (PARTIE DE PAUME CONCERNÉE PAR LE RELEVÉ)	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE DEFINITION (RESERVÉES EN VUE D'UNE DÉFINITION ULTÉRIEURE)	—	—	—	—	—	—
COM	F	15.020	COMMENT (COMMENTAIRE)	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE DEFINITION (RÉSERVÉES EN VUE D'UNE DÉFINITION ULTÉRIEURE)	—	—	—	—	—	—
UDF	F	15.200 15.998	USER-DEFINED FIELDS (ZONES DÉFINIES PAR L'UTILISATEUR)	—	—	—	—	—	—
DAT	O	15.999	IMAGE DATA (DONNÉES CONCERNANT L'IMAGE)	B	2	—	1	1	—

Tableau 9: méthode d'obtention des images d'empreintes palmaires — codes autorisés et signification

Description	Code
Numérisation directe	10
Numérisation à partir d'un support	11
Trace latente	12
Reproduction manuelle agrandie de trace latente	13
Photo argentique de trace latente	14
Transfert de trace latente	15

8.1.11. Zone 15.011: CGA (Compression Algorithm — algorithme de compression)

Cette zone ASCII obligatoire indique l'algorithme utilisé pour compresser les images à niveaux de gris. NONE signifie que les données contenues dans cet enregistrement ne sont pas compressées. Lorsqu'on souhaite compresser les images, cette zone spécifie la méthode retenue pour la compression des images d'empreintes décadactylaires. Les codes de compression valables figurent à l'annexe 7.

8.1.12. Zone 15.012: BPX (Bits Per Pixel — nombre de bits par pixel)

Cette zone ASCII obligatoire spécifie le nombre de bits utilisés pour représenter un pixel. Il convient d'y indiquer «8» pour les valeurs de niveaux de gris normales comprises entre 0 et 255. Toute valeur supérieure à 8 représente un pixel en niveaux de gris de plus grande précision. Toute valeur inférieure à 8 représente un pixel en niveaux de gris de moins grande précision.

Tableau 10: codes des différentes parties de la paume et dimensions de l'image

Partie de paume concernée par le relevé	Code	Dimension maximale de l'image (mm^2)	Largeur maximale (mm)	Longueur maximale (mm)
Paume non identifiée	20	28 387	139,7	203,2
Paume droite entière	21	28 387	139,7	203,2
Paume droite	22	5 645	44,5	127,0
Paume gauche entière	23	28 387	139,7	203,2
Paume gauche	24	5 645	44,5	127,0
Partie inférieure de la paume droite	25	19 516	139,7	139,7
Partie supérieure de la paume droite	26	19 516	139,7	139,7
Partie inférieure de la paume gauche	27	19 516	139,7	139,7
Partie supérieure de la paume gauche	28	19 516	139,7	139,7
Autre, main droite	29	28 387	139,7	203,2
Autre, main gauche	30	28 387	139,7	203,2

8.1.13. Zone 15.013: PLP (Palmprint Position — partie de paume concernée par le relevé)

Cette zone balisée obligatoire spécifie la partie de paume représentée par l'image. Elle contient l'un des codes décimaux du tableau 10 correspondant de façon certaine ou la plus probable à la partie de paume concernée, et se présentant sous la forme d'une sous-zone ASCII à deux caractères. Le tableau 10 précise également la surface maximale pouvant être transmise pour chacune des parties de paume.

8.1.14. Zones 15.014 à 019: RSV (Reserved for Future Definition — réservées en vue d'une définition ultérieure)

Les zones concernées seront définies dans les futures révisions de la présente norme. Aucune d'entre elles ne doit être utilisée dans le cadre de la présente révision. Si l'une d'elles est spécifiée, elle ne doit pas être prise en compte.

8.1.15. Zone 15.020: COM (Comment — commentaire)

Cette zone facultative peut être utilisée pour ajouter des commentaires ou du texte ASCII aux données concernant l'image d'empreinte palmaire.

8.1.16. Zones 15.021 à 199: RSV (Reserved for Future Definition — réservées en vue d'une définition ultérieure)

Les zones concernées seront définies dans les futures révisions de la présente norme. Aucune d'entre elles ne doit être utilisée dans le cadre de la présente révision. Si l'une d'elles est spécifiée, elle ne doit pas être prise en compte.

8.1.17. Zones 15.200 à 998: UDF (User-Defined Fields — zones définies par l'utilisateur)

Ces zones peuvent être définies par l'utilisateur et seront utilisées en fonction des nécessités ultérieures. Leur taille et leur contenu sont fixés par l'utilisateur, en accord avec le service destinataire. Si elles sont spécifiées, elles contiennent du texte ASCII.

8.1.18. Zone 15.999: DAT (Image Data — données concernant l'image)

Cette zone contient toutes les indications relatives à une image acquise d'empreinte palmaire. Il convient de toujours lui attribuer le numéro 999. Elle doit toujours être la dernière zone de l'enregistrement. Par exemple, «15.999:» est suivi de données binaires sur l'image. Chaque pixel des données d'une image à niveaux de gris non compressée est normalement décrit sur les huit bits (256 niveaux de gris) d'un seul octet. Si la zone 15.012 (BPX) contient une valeur inférieure ou supérieure à 8, le nombre d'octets requis pour décrire un pixel sera différent. Si l'image est compressée, les données relatives aux pixels seront compressées au moyen de la technique spécifiée dans la zone CGA.

8.2. *Fin de l'enregistrement logique de type 15*

Pour des raisons de cohérence, le dernier octet de la zone 15.999 doit être séparé de l'enregistrement logique suivant par le séparateur FS. Ce séparateur doit être pris en compte dans la zone LEN de l'enregistrement de type 15.

8.3. *Enregistrements supplémentaires*

Le fichier peut contenir des enregistrements de type 15 supplémentaires. À chaque image d'empreinte palmaire supplémentaire doit correspondre un enregistrement logique de type 15 séparé du suivant par un caractère FS.

Tableau 11: nombre maximal de propositions acceptées pour vérification par transmission

Type de recherche FAED	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Nombre maximal de propositions	1	10	5	5	5	5	5

Types de recherche:

TP/TP: empreinte décadactylaire par rapport à une empreinte décadactylaire

LT/TP: empreinte digitale latente par rapport à une empreinte décadactylaire

LP/PP: empreinte palmaire latente par rapport à une empreinte palmaire

TP/UL: empreinte décadactylaire par rapport à une empreinte digitale latente non résolue

LT/UL: empreinte digitale latente par rapport à une empreinte digitale latente non résolue

PP/ULP: empreinte palmaire par rapport à une empreinte palmaire latente non résolue

LP/ULP: empreinte palmaire latente par rapport à une empreinte palmaire latente non résolue

9. ***Appendices au chapitre 2 (échange de données dactyloscopiques)***

9.1. *Appendice 1: codes de séparation ASCII*

ASCII	Position ([1])	Description
LF	1/10	Sépare les codes d'erreur dans la zone 2074
FS	1/12	Sépare les enregistrements logiques d'un fichier
GS	1/13	Sépare les zones d'un enregistrement logique
RS	1/14	Sépare les sous-zones d'une zone
US	1/15	Sépare les différents éléments d'information d'une zone ou d'une sous-zone

([1]) Position telle que définie dans la norme ASCII.

9.2. *Appendice 2: calcul du caractère de contrôle alphanumérique*

Pour les zones TCN et TCR (1.09 et 1.10):

Le nombre correspondant au caractère de contrôle est généré par la formule qui suit:

(AA * 10^{8} + SSSSSSSS) modulo 23

dans laquelle AA et SSSSSSSS sont les valeurs numériques des deux derniers chiffres de l'année et du numéro de série, respectivement.

Le caractère de contrôle lui-même est ensuite généré à partir du tableau de correspondance figurant ci-dessous.

Pour la zone CRO (2010):

Le nombre correspondant au caractère de contrôle est généré par la formule qui suit:

(AA * 10^6 + NNNNNN) modulo 23

dans laquelle AA et NNNNNNNN sont les valeurs numériques des deux derniers chiffres de l'année et du numéro de série, respectivement.

Le caractère de contrôle lui-même est ensuite généré à partir du tableau de correspondance figurant ci-dessous.

Tableau de correspondance des caractères de contrôle

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3. *Appendice 3: codage de caractères*

Code ANSI à 7 bits pour l'échange d'informations

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	»	#	$	%	&	‘
40	(	)	*	+	,	—	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

9.4. *Appendice 4: résumé des opérations*

Enregistrement de type 1 (obligatoire)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Où:

O = optional (facultatif); M = mandatory (obligatoire); C = à condition que l'opération soit une réponse au service d'origine.

Enregistrements de type 2 (obligatoires)

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Où:

O = optional (facultatif); M = mandatory (obligatoire); C = à condition que des données soient disponibles.

*) = si les données sont transmises en application de la législation nationale (en dehors du champ d'application de la décision 2008/615/JAI)

9.5. *Appendice 5: définition des enregistrements de type 1*

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1 001:230{GS}
VER	M	1.002	Version Number	N	1 002:0300{GS}
CNT	M	1.003	File Content	N	1 003:1{US}15{RS}2{US}00{RS}4 {US}01{RS}4{US}02 {RS}4{US}03 {RS}4{US}04 {RS}4{US}05{RS}4 {US}06 {RS}4{US}07{RS}4{US}08 {RS}4{US}09{RS}4{US}10 {RS}4 {US}11{RS}4{US}12 {RS}4{US}13 {RS}4{US}14 {GS}
TOT	M	1.004	Type of Transaction	A	1 004:CPS{GS}
DAT	M	1.005	Date	N	1 005:20050101{GS}
PRY	M	1.006	Priority	N	1 006:4{GS}
DAI	M	1.007	Destination Agency	1*	1 007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1 008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1 009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1 010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1 011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1 012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1 014:20050101125959Z

Dans la colonne «Condition»: O = optional (facultatif); M = mandatory (obligatoire); C = conditionnel.

Dans la colonne «Character Type»: A = alphabétique, N = numérique, B = binaire

1* Les caractères autorisés pour le nom du service sont [«0..9», «A..Z», «a..z», «_»,».», « «, «-»]

9.6. *Appendice 6: définition des enregistrements de type 2*

Tableau A.6.1: opérations CPS et PMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2 001:909{GS}
IDC	M	2.002	Image Designation Character	N	2 002:00{GS}
SYS	M	2.003	System Information	N	2 003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2 010:DE/E999999999 {GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
INF	O	2.063	Additional Information	1*	2 063:Additional Information 123 {GS}
ENC	M	2.320	Expected Number of Candidates	N	2 320:1{GS}

Tableau A.6.2: opération SRE

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2 001:909{GS}
IDC	M	2.002	Image Designation Character	N	2 002:00{GS}
SYS	M	2.003	System Information	N	2 003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2 010:NL/2222222222 {GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2 012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2 013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2 014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2 015:A{GS}
INF	O	2.063	Additional Information	1*	2 063:Additional Information 123 {GS}
RLS	M	2.064	Respondents List	AN	2 064:CPS{RS}I{RS}001/001{RS} 999999{GS}

Tableau A.6.3: opération ERR

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2 001:909{GS}
IDC	M	2.002	Image Designation Character	N	2 002:00{GS}
SYS	M	2.003	System Information	N	2 003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2 012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2 013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2 014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2 015:A{GS}
INF	O	2.063	Additional Information	1*	2 063:Additional Information 123 {GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
ERM	M	2.074	Status/Error Message Field	AN	2 074: 201: IDC - 1 FIELD 1 009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2 003 INVALID SYSTEM INFORMATION {GS}

Tableau A.6.4: opérations MPS MMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2 001:909{GS}
IDC	M	2.002	Image Designation Character	N	2 002:00{GS}
SYS	M	2.003	System Information	N	2 003:0422{GS}
CNO	M	2.007	Case Number	AN	2 007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2 008:0001{GS}
MID	C	2.009	Latent Identifier	A	2 009:A{GS}
INF	O	2.063	Additional Information	1*	2 063:Additional Information 123 {GS}
ENC	M	2.320	Expected Number of Candidates	N	2 320:1{GS}

Dans la colonne «Condition»: O = optional (facultatif); M = mandatory (obligatoire); C = conditionnel.

Dans la colonne «Character Type»: A = alphabétique, N = numérique, B = binaire

1* Les caractères autorisés sont [«0..9», «A..Z», «a..z», «_»,».», « «, «-»,»,»]

9.7. *Appendice 7: codes des algorithmes de compression (images à niveaux de gris)*

Compression	Value	Remarks
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated December 19, 1997	WSQ	Algorithm to be used for the compression of grayscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500dpi.
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of grayscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi

9.8. *Appendice 8: spécifications pour le courrier électronique*

Pour améliorer le déroulement des opérations au niveau interne, le sujet d'un courrier électronique dans le cadre d'une opération PRUEM doit être le code pays (CC) de l'État membre qui envoie le message et le type d'opération (zone TOT 1 004).

Format: CC/*type d'opération*

Exemple: «DE/CPS»

Le corps du message peut être vide.

CHAPITRE 3: **Échange de données relatives à l'immatriculation des véhicules**

1. ***Ensemble commun de données aux fins de la consultation automatisée de données relatives à l'immatriculation des véhicules***

1.1. *Définitions*

Les définitions qui suivent s'appliquent aux éléments de données obligatoires et facultatifs au titre de l'enregistrement 16, paragraphe 4:

Obligatoire (O):

L'élément de donnée doit être communiqué lorsque l'information est disponible dans le registre national d'un État membre. Par conséquent, il est obligatoire d'échanger l'information en question lorsqu'elle est disponible.

Facultatif (F):

L'élément de donnée peut être communiqué lorsque l'information est disponible dans le registre national d'un État membre. Par conséquent, il n'y a aucune obligation d'échanger l'information en question, même lorsqu'elle est disponible.

Une mention (Y) indique si un élément figurant dans l'ensemble de données est spécifiquement identifié comme important dans le cadre de la décision 2008/615/JAI.

1.2. *Recherche concernant un véhicule, un propriétaire ou un détenteur*

1.2.1. Éléments déclenchant la recherche

Il existe deux façons de rechercher l'information définie dans le paragraphe suivant:

— par numéro de châssis du véhicule, date et heure de référence (facultatif),

— par numéro de la plaque d'immatriculation, numéro de châssis du véhicule (facultatif) et date et heure de référence (facultatif).

Ces critères de recherche permettent de trouver les informations relatives à un ou, parfois, à plusieurs véhicules. Si des informations ne sont disponibles que pour un seul véhicule, tous les éléments sont transmis dans une seule réponse. Si plus d'un véhicule est trouvé, l'État membre requis lui-même peut déterminer quels sont les éléments qui seront transmis: l'ensemble des éléments ou uniquement ceux qui permettent d'affiner la recherche (par exemple, pour protéger la vie privée ou pour des raisons d'efficacité).

Les éléments nécessaires afin d'affiner la recherche sont énumérés au point 1.2.2.1. L'ensemble des informations figurent au point 1.2.2.2.

Une recherche par numéro d'identification du véhicule, date et heure de référence peut être effectuée dans un des États membres participants ou dans leur ensemble.

Une recherche par numéro d'immatriculation, date et heure de référence doit être effectuée dans un seul État membre.

Même si, normalement, on a recours pour la recherche à la date et à l'heure réelles, il est également possible d'effectuer une recherche avec une date et une heure de référence situées dans le passé. Lorsqu'une recherche est effectuée avec une date et une heure de référence situées dans le passé et qu'un historique n'est pas disponible dans le registre de l'État membre concerné, les informations de ce type n'étant pas consignées, l'information peut être transmise accompagnée d'une mention selon laquelle il s'agit d'une information réelle.

1.2.2. Ensemble des éléments

1.2.2.1. Éléments à transmettre nécessaires pour affiner la recherche

Élément	O/F [1]	Remarques	Prüm Y/N [2]
Données relatives aux véhicules			
Numéro d'immatriculation	O		Y
Numéro d'identification du véhicule	O		Y
Pays d'immatriculation	O		Y
Marque	O	[D.1 [3]] par exemple Ford, Opel, Renault etc.	Y
Dénomination commerciale du véhicule	O	(D.3) par exemple Focus, Astra, Megane	Y

Élément	O/F (1)	Remarques	Prüm Y/N (2)
Code catégorie UE	O	J) Cyclomoteur, moto, voiture, etc.	Y

(1) O = obligatoire lorsque les informations en question sont disponibles dans le registre national; F = facultatif.
(2) Tous les attributs spécifiquement attribués par les États membres sont indiqués par un O.
(3) Abréviations des documents d'immatriculation harmonisés; voir la directive 1999/37/CE du Conseil du 29 avril 1999.

1.2.2.2. Ensemble complet des données

Élément	O/F (1)	Remarques	Prüm Y/N
Données relatives aux détenteurs du véhicule		[C.1 (2)] Données correspondant au titulaire du certificat d'immatriculation concerné.	
Nom (raison sociale) du titulaire du certificat d'immatriculation	O	(C.1.1) Utiliser des champs séparés pour le nom de famille, les titres, etc. Le nom sera communiqué dans un format imprimable	Y
Prénom	O	(C.1.2) Utiliser des champs séparés pour le ou les prénoms et les initiales. Le nom sera communiqué dans un format imprimable	Y
Adresse	O	(C.1.3) Utiliser des champs séparés pour la rue, le numéro de maison, le code postal, le lieu de résidence, le pays du lieu de résidence, etc. L'adresse sera communiquée dans un format imprimable	Y
Sexe	O	Masculin, féminin	Y
Date de naissance	O		Y
Entité juridique	O	Personne physique, association, société, firme, etc.	Y
Lieu de naissance	F		Y
Identifiant	F	Identifiant unique pour la personne ou la société	N
Type d'identifiant	F	Type d'identifiant (par exemple, numéro de passeport)	N
Date de début de détention	F	Date de début de détention du véhicule. Cette date est souvent celle qui est inscrite sous la mention (I) du certificat d'immatriculation du véhicule	N
Date de fin de détention	F	Date de fin de détention du véhicule	N
Type de détenteur	F	Si le véhicule n'a pas de propriétaire (C.2), mention relative au fait que le détenteur du certificat d'immatriculation: — est le propriétaire du véhicule — n'est pas le propriétaire du véhicule — n'est pas identifié par le certificat d'immatriculation en tant que propriétaire du véhicule	N
Données relatives aux propriétaires des véhicules		(C.2)	
Nom ou raison sociale	O	(C.2.1)	Y
Prénom	O	(C.2.2)	Y

Élément	O/F [1]	Remarques	Prüm Y/N
Adresse	O	(C.2.3)	Y
Sexe	O	Masculin, féminin	Y
Date de naissance	O		Y
Entité juridique	O	Personne physique, association, société, firme, etc.	Y
Lieu de naissance	F		Y
Identifiant	F	Identifiant unique pour la personne ou la société	N
Type d'identifiant	F	Type d'identifiant (par exemple, numéro de passeport)	N
Date de début de possession	F	Date de début de la possession du véhicule	N
Date de fin de possession	F	Date de fin de la possession du véhicule	N
Données relatives aux véhicules			
Numéro du certificat d'immatriculation	O		Y
Numéro d'identification du véhicule	O		Y
Pays d'immatriculation	O		Y
Marque	O	(D.1) par exemple, Ford, Opel, Renault etc.	Y
Dénomination commerciale du véhicule	O	(D.3) par exemple, Focus, Astra, Megane	Y
Code catégorie UE	O	J) Cyclomoteur, moto, voiture, etc.	Y
Date de la première immatriculation	O	B) Date de la première immatriculation du véhicule, où que ce soit dans le monde	Y
Date (réelle) de début de l'immatriculation	O	I) Date de l'immatriculation à laquelle se réfère le certificat spécifique du véhicule	Y
Date de fin de l'immatriculation	O	Date de fin de l'immatriculation mentionnée dans le certificat spécifique du véhicule. Il se peut que cette date indique la période de validité telle que mentionnée sur le document, si elle n'est pas à durée indéterminée (abréviation document = H).	Y
Statut	O	Mis au rebut, volé, exporté, etc.	Y
Date de début du statut	O		Y
Date de fin du statut	F		N
kW	F	(P.2)	Y
Capacité	F	(P.1)	Y
Type de numéro de plaque	F	Normal, transit, etc.	Y
Id. 1 document véhicule	F	Premier identifiant unique, tel qu'il figure sur le document du véhicule	Y
Id. 2 document véhicule [3]	F	Deuxième identifiant unique, tel qu'il figure sur le document du véhicule	Y
Informations en matière d'assurance			
Nom de l'assureur	F		Y
Date de début de la couverture	F		Y
Date de fin de la couverture	F		Y
Adresse	F		Y
Numéro d'assurance	F		Y

Élément	O/F (1)	Remarques	Prüm Y/N
Numéro d'identification	F	Identifiant unique de l'assureur.	N
Type d'identifiant	F	Par exemple, numéro attribué par la chambre de commerce.	N

(1) O = obligatoire lorsque les informations en question sont disponibles dans le registre national; F = facultatif.
(2) Abréviations des documents d'immatriculation harmonisés; voir la directive 1999/37/CE du Conseil du 29 avril 1999.
(3) Au Luxembourg, deux documents d'immatriculation distincts sont utilisés.

2. ***Sécurité des données***

2.1. *Aperçu*

Le logiciel Eucaris gère les communications sécurisées vers les autres États membres et communique, par le langage XML, avec les systèmes finaux plus anciens des États membres. Les États membres échangent des messages en les transmettant directement au destinataire. Les centres de données des États membres sont reliés au réseau TESTA de l'Union européenne.

Les messages XML envoyés sur le réseau sont cryptés. Le protocole SSL (Secure Sockets Layer) est utilisé à cet effet. Les messages sont expédiés au site destinataire en format texte selon la norme XML, la connexion entre l'application et l'unité finale se trouvant dans un environnement sécurisé.

Une application client est fournie, qui peut être utilisée pour effectuer des recherches dans le registre de l'État membre lui-même ou celui des autres États membres. Les clients sont identifiés par un nom d'utilisateur et un mot de passe, ou un certificat de client. Il revient à chaque État membre de décider si la connexion de chaque utilisateur est cryptée.

2.2. *Caractéristiques de sécurité liées à l'échange de messages*

La sécurité repose sur une combinaison de signatures HTTPS et XML. Cette approche consiste à signer en XML tous les messages envoyés au serveur et permet d'authentifier l'expéditeur du message en vérifiant la signature. Le protocole SSL unilatéral (certificat côté serveur uniquement) est utilisé pour garantir la confidentialité et l'intégrité du message en transit et assurer une protection contre les attaques par effacement, insertion ou nouveau jeu (replay). On a recours à la signature XML au lieu d'un logiciel sur mesure pour mettre en œuvre le protocole SSL bilatéral. La signature XML est plus proche de l'architecture des services web que le protocole SSL bilatéral et, par conséquent, plus stratégique.

Si la signature XML peut être mise en œuvre de plusieurs façons, l'approche retenue est de l'utiliser dans le cadre du protocole WS-Security. Ce protocole prévoit des spécifications pour l'utilisation de la signature XML. Le protocole WS-Security étant fondé sur la norme SOAP, il est logique de se conformer à cette dernière autant que possible.

2.3. *Caractéristiques de sécurité non liées à l'échange de messages*

2.3.1. Authentification des utilisateurs

Les utilisateurs de l'application web Eucaris s'authentifient par un nom d'utilisateur et un mot de passe. L'authentification standard de Windows étant utilisée, les États membres peuvent renforcer le niveau d'authentification des utilisateurs, au besoin, grâce à des certificats côté client.

2.3.2. Rôles des utilisateurs

L'application Eucaris prévoit différents rôles pour les utilisateurs. À chaque groupe de services correspond une autorisation spécifique. Par exemple, les utilisateurs exclusivement autorisés à utiliser la fonctionnalité «Traité Eucaris» ne peuvent utiliser la fonctionnalité «Prüm». Les services réservés aux administrateurs sont séparés des rôles normalement dévolus aux utilisateurs finaux.

2.3.3. Historique et traçabilité de l'échange de messages

L'application Eucaris facilite l'enregistrement d'un historique de tous les types de messages. Une fonction d'administration permet à l'administrateur national de déterminer quels messages sont enregistrés dans l'historique: demandes des utilisateurs finaux, demandes provenant des États membres, informations extraites des registres nationaux, etc.

Pour l'enregistrement de ces données dans l'historique, l'application peut être configurée pour utiliser soit une base de données interne, soit une base de données externe (Oracle). La décision concernant les messages à enregistrer dans l'historique dépend des possibilités en la matière des systèmes plus anciens situés ailleurs, ainsi que des applications clients connectées.

L'en-tête de chaque message contient des informations sur l'État membre requérant, le service requérant de cet État membre ainsi que l'utilisateur concerné. Le motif de la demande est également indiqué.

Grâce à ces historiques combinés, tant dans l'État requérant que dans l'État qui répond, il est possible d'assurer une traçabilité complète de tout échange de messages (par exemple, à la demande d'une personne concernée).

L'enregistrement de l'historique est configuré à partir du client web Eucaris (menu administration, configuration de l'historique). La fonctionnalité elle-même est mise en œuvre par le noyau système. Lorsque l'historique est activé, le message complet (en-tête et corps) est stocké dans un enregistrement. Le niveau de précision de l'historique peut être paramétré par service et par type de messages passant par le noyau système.

Niveaux de précision de l'historique

Les niveaux qui suivent peuvent être définis:

Privé: le message est enregistré. L'enregistrement n'est pas disponible pour le service d'extraction des enregistrements, mais exclusivement au niveau national, à des fins d'audit et de résolution de problèmes.

Aucun: le message n'est pas enregistré.

Types de message

L'échange d'informations entre États membres consiste en plusieurs messages, dont la figure ci-dessous propose une représentation schématique.

Les types de messages possibles (dans la figure, pour le noyau système Eucaris d'un État membre X) sont les suivants:

1) requête adressée au noyau système par un client;

2) requête adressée à un autre État membre par le noyau système de l'État membre X;

3) requête adressée au noyau système de l'État membre X par le noyau système d'un autre État membre;

4) requête adressée à un registre ancien par le noyau système;

5) requête adressée au noyau système par un registre ancien;

6) réponse du noyau système à une requête adressée par un client;

7) réponse d'un autre État membre à une requête adressée par le noyau système de l'État membre X;

8) réponse du noyau système de l'État membre X à une requête adressée par un autre État membre;

9) réponse d'un registre ancien à une requête adressée par le noyau système;

10) réponse du noyau système à une requête adressée par un registre ancien;

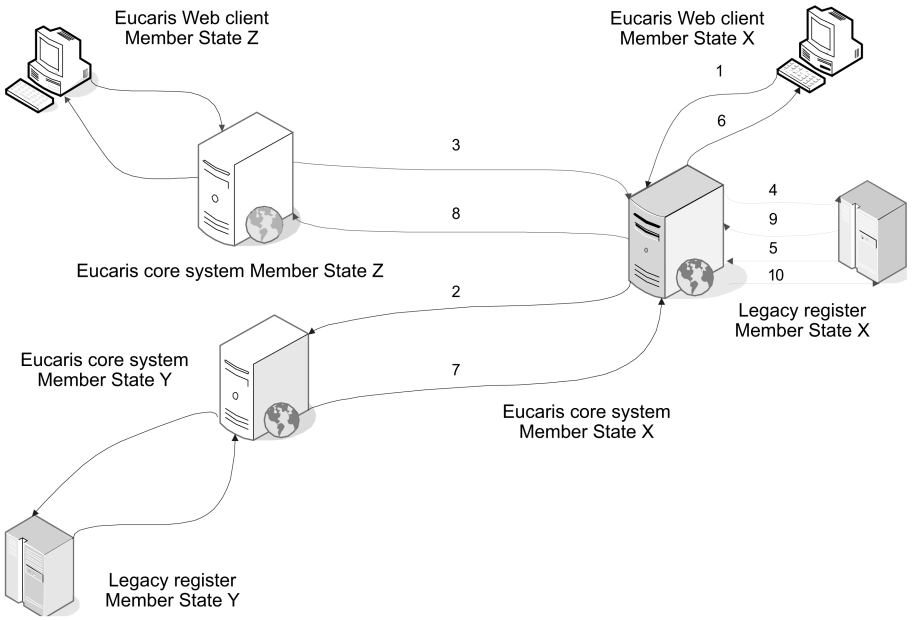
Les échanges d'informations qui suivent sont illustrés dans la figure:

— demande d'informations adressée par l'État membre X à l'État membre Y — flèches bleues. La demande et la réponse consistent en messages de types 1, 2, 7 et 6, respectivement,

— demande d'informations adressée par l'État membre Z à l'État membre X — flèches rouges. La demande et la réponse consistent en messages de types 3, 4, 9 et 8, respectivement,

— demande d'informations adressée par un registre ancien à son noyau système (ce trajet recouvre en outre une demande adressée par un client personnalisé en amont d'un registre ancien) — flèches vertes. La demande et la réponse consistent en messages de types 5 et 10, respectivement.

Figure: types de messages pour l'enregistrement de l'historique.



2.3.4. Module matériel de sécurité (HSM)

Un tel module de sécurité n'est pas utilisé.

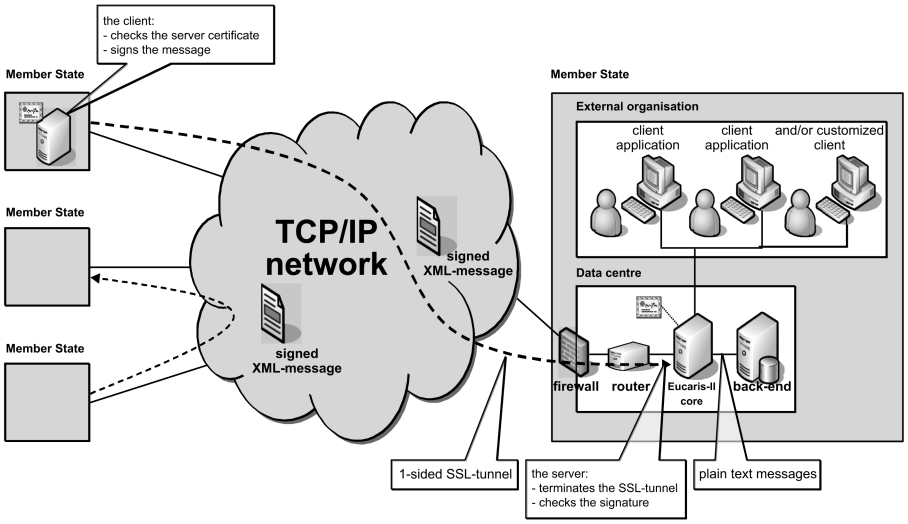
Un HSM assure une bonne protection de la clé utilisée pour signer les messages et identifier les serveurs. S'il est vrai que la sécurité s'en trouve renforcée, le HSM coûte cher à l'achat et à l'entretien et il n'est pas nécessaire d'opter pour un HSM à la norme FIPS 140-2 de niveau 2 ou 3. Puisque c'est un réseau fermé qui est mis en œuvre, ce qui est une façon efficace de limiter les risques, il est décidé de ne pas recourir initialement à un HSM. Si un tel module s'avère nécessaire, par exemple pour obtenir une homologation, il peut être ajouté à l'architecture.

3. *Conditions techniques de l'échange de données*

3.1. *Description générale de l'application Eucaris*

3.1.1. Aperçu

L'application Eucaris relie tous les États membres participants par un réseau maillé dans lequel chaque État membre peut communiquer directement avec les autres. Aucun élément central n'est nécessaire pour que la communication soit établie. L'application Eucaris gère la communication sécurisée vers les autres États membres et communique avec les unités finales anciennes des États membres au moyen du langage XML. Le diagramme qui suit illustre cette architecture.



Les États membres échangent des messages en les envoyant directement au destinataire. Le centre de données d'un État membre est relié au réseau utilisé pour l'échange de messages (TESTA). Les États membres se connectent au réseau TESTA via leur passerelle nationale. Un pare-feu est utilisé pour la connexion au réseau, et un routeur relie l'application Eucaris au pare-feu. Un certificat est délivré soit par le routeur, soit par l'application Eucaris, selon la solution retenue pour protéger les messages.

Les États membres peuvent utiliser l'application client fournie pour effectuer des recherches dans leur propre registre ou ceux des autres États membres. L'application client se connecte à Eucaris. Les clients sont identifiés par nom d'utilisateur et mot de passe, ou par un certificat de client. La connexion avec un utilisateur dans un service externe (par exemple, la police) peut être cryptée; il revient à chaque État membre de prendre une décision à ce sujet.

3.1.2. Champ d'application du système

Le champ d'application d'Eucaris est limité aux processus liés à l'échange d'informations entre les autorités chargées de l'immatriculation dans les États membres et à une présentation sommaire des informations en question. Les procédures et les processus automatisés dans lesquels les informations doivent être utilisées ne relèvent pas du champ d'application du système.

Les États membres peuvent choisir soit de recourir à la fonctionnalité du client Eucaris, soit de créer leur propre application client. Le tableau ci-dessous décrit les aspects du système Eucaris qui sont d'utilisation obligatoire ou recommandée et lesquels sont facultatifs et/ou de détermination libre par les États membres.

EUCARIS aspects	M/O [1]	Remark
Network concept	M	The concept is an «any-to-any» communication.
Physical network	M	TESTA
Core application	M	The core application of EUCARIS has to be used to connect to the other Member States. The following functionality is offered by the core: — Encrypting and signing of the messages; — Checking of the identity of the sender; — Authorization of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the EUCARIS II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the EUCARIS organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the EUCARIS organisation and this Council Decision. The specifications can only be changed by the EUCARIS organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the EUCARIS organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

[1] M = (mandatory) utilisation ou respect obligatoire; O = (optional) utilisation ou respect facultatif.

3.2. *Exigences fonctionnelles et non fonctionnelles*

3.2.1. Fonctionnalité générique

La présente partie décrit en termes généraux les principales fonctions génériques.

Nº	Description
1.	Le système permet aux autorités chargées de l'immatriculation, dans les États membres, d'échanger des messages de demande et des réponses d'une façon interactive.
2.	Le système comprend une application client qui permet aux utilisateurs finaux d'envoyer leurs demandes et qui présente les informations reçues en réponse à des fins de traitement manuel.
3.	Le système facilite la diffusion et permet à un État membre d'envoyer une demande à tous les autres. L'application centrale regroupe les réponses reçues en une seule, qui est envoyée à l'application client (cette fonctionnalité s'appelle «demande de renseignements à plusieurs pays»).
4.	Le système peut gérer différents types de messages. Les rôles des utilisateurs, l'autorisation, le routage, la signature et l'enregistrement dans l'historique sont des paramètres définis spécifiquement par service.
5.	Le système permet aux États membres d'échanger des messages groupés ou des messages contenant de nombreuses demandes ou réponses. Ces messages sont traités d'une façon asynchrone.
6.	Le système place les messages asynchrones dans une file d'attente si l'État membre est temporairement indisponible et garantit que les messages seront effectivement acheminés dès que le destinataire sera de nouveau disponible.
7.	Le système stocke les messages asynchrones reçus jusqu'à ce qu'ils puissent être traités.
8.	Le système ne donne accès qu'aux applications Eucaris des autres États membres, et non à des services particuliers dans ces États membres, ce qui signifie que chaque autorité chargée de l'immatriculation fait office de passerelle unique entre ses utilisateurs finaux au niveau national et les autorités correspondantes dans les autres États membres.
9.	Il est possible de créer des comptes d'utilisateurs de différents États membres sur un serveur Eucaris unique et de leur attribuer des autorisations sur la base des permissions prévues dans l'État membre concerné.
10.	Chaque message inclut des informations sur l'État membre requérant, le service et l'utilisateur final.
11.	Le système facilite l'enregistrement d'un historique de l'échange de messages entre les différents États membres ainsi qu'entre l'application centrale et les systèmes nationaux d'immatriculation.
12.	Le système permet à un secrétaire, c'est-à-dire un service ou un État membre désigné spécifiquement pour remplir ce rôle, de collecter des informations tirées de l'historique sur les messages envoyés et reçus par tous les États membres participants, de façon à produire des rapports statistiques.
13.	Chaque État membre indique quelles informations enregistrées dans l'historique sont mises à la disposition du secrétaire, et lesquelles sont «privées».
14.	Le système permet aux administrateurs nationaux de chaque État membre d'extraire des données statistiques sur l'utilisation.
15.	Le système permet d'ajouter de nouveaux États membres par des opérations administratives simples.

3.2.2. Facilité d'utilisation

Nº	Description
16.	Le système comporte une interface pour le traitement automatisé des messages par les unités finales ou les systèmes plus anciens et permet l'intégration de l'interface utilisateur dans ces systèmes (interfaces personnalisées).
17.	Le système est d'un apprentissage simple, ne nécessite aucune explication et contient des textes d'aide.
18.	Le système est documenté pour assister les États membres en ce qui concerne l'intégration, les activités opérationnelles et l'entretien ultérieur (par exemple, guides de référence, documentation fonctionnelle et technique, mode d'emploi…).
19.	L'interface utilisateur est plurilingue, l'utilisateur final pouvant sélectionner la langue de son choix.
20.	L'interface utilisateur prévoit la possibilité pour un administrateur local de traduire dans une langue nationale tant les éléments qui apparaissent à l'écran que les informations codées.

3.2.3. Fiabilité

Nº	Description
21.	Le système opérationnel est conçu pour être robuste et fiable, pour tolérer les erreurs commises par les opérateurs et pour se relancer sans problème en cas de coupure de courant ou d'autres incidents. Il doit être possible de relancer le système sans perte de données ou au prix de pertes très limitées.
22.	Le système doit produire des résultats constants et reproductibles.
23.	Le système a été conçu dans un souci de fiabilité. Il est possible de le mettre en œuvre dans une configuration garantissant une disponibilité de 98 % (au moyen de la redondance, de serveurs auxiliaires, etc.) pour chaque communication bilatérale.
24.	Il est possible d'utiliser une partie du système, même en cas d'indisponibilité de certaines composantes (par exemple, si l'État membre C est indisponible, les États membres A et B peuvent toujours communiquer). Le nombre de points faibles dans la chaîne d'information doit être ramené au minimum.
25.	Le temps de réparation après un incident grave devrait être inférieur à un jour. Il devrait être possible de limiter la durée d'indisponibilité en faisant appel à un soutien à distance fourni, par exemple, par un service central.

3.2.4. Performance

Nº	Description
26.	Le système peut être utilisé 24 heures sur 24 et 7 jours sur 7. La même exigence s'applique aux systèmes plus anciens des États membres.
27.	Le système répond rapidement aux demandes des utilisateurs, indépendamment des tâches d'arrière-plan éventuellement en cours. La même exigence s'applique aux systèmes plus anciens des États membres, pour que le temps de réponse soit acceptable. Un délai de réponse de 10 secondes au plus par demande est acceptable.
28.	Le système a été conçu comme un environnement multiutilisateur et de telle façon que les tâches d'arrière-plan puissent se poursuivre pendant que l'utilisateur accomplit des tâches d'avant-plan.
29.	Le système est conçu pour être modulable et pouvoir s'adapter à l'augmentation éventuelle du nombre de messages lorsqu'une nouvelle fonctionnalité, de nouveaux services ou de nouveaux États membres sont ajoutés.

3.2.5. Sécurité

Nº	Description
30.	Le système est adapté (par exemple, en ce qui concerne les mesures de sécurité) à l'échange de messages contenant des données sensibles, à caractère personnel ou concernant la vie privée (par exemple, propriétaires ou détenteurs de véhicules), classifiées au niveau UE restreint.
31.	Le système est configuré de façon à empêcher tout accès non autorisé aux données.
32.	Le système dispose d'un service permettant de gérer les droits et les permissions des utilisateurs finaux au niveau national.
33.	Les États membres peuvent vérifier l'identité de l'expéditeur (au niveau des États membres) grâce à la signature XML.
34.	Les États membres doivent expressément autoriser les autres États membres à demander des informations spécifiques.
35.	Le système prévoit, au niveau de l'application, une politique exhaustive de sécurité et de cryptage conforme au niveau de sécurité nécessaire dans de tels environnements. Le caractère exclusif et l'intégrité des informations sont garantis par l'utilisation de la signature XML et de tunnels chiffrés avec SSL.
36.	La traçabilité de tout échange de message est assurée grâce à un historique.
37.	Une protection est fournie contre les attaques par effacement (un tiers efface un message), nouveau jeu (un tiers répète un message) ou insertion (un tiers insère un message).
38.	Le système utilise des certificats délivrés par un tiers de confiance (TC).
39.	Le système peut gérer plusieurs certificats par État membre, selon le type de message ou de service.

Nº	Description
40.	Les mesures de sécurité prises au niveau de l'application suffisent pour qu'il soit possible de recourir à des réseaux non homologués.
41.	Le système peut utiliser des techniques nouvelles en matière de sécurité, par exemple un pare-feu XML.

3.2.6. Adaptabilité

Nº	Description
42.	Le système est extensible par de nouveaux types de messages et de nouvelles fonctionnalités. Le coût des adaptations à apporter est faible, le développement des composantes de l'application étant centralisé.
43.	Les États membres peuvent définir de nouveaux types de messages à usage bilatéral. Tous les États membres ne sont pas obligés d'accepter tous les types de messages.

3.2.7. Assistance et maintenance

Nº	Description
44.	Le système dispose de fonctions de surveillance à l'usage d'un service central et/ou d'opérateurs en ce qui concerne le réseau et les serveurs situés dans les différents États membres.
45.	Le système dispose de fonctions permettant de fournir une assistance à distance, à partir d'un service central.
46.	Le système dispose de fonctions permettant d'analyser les problèmes.
47.	Le système peut être étendu pour couvrir de nouveaux États membres.
48.	L'application peut être installée facilement par du personnel disposant de compétences et d'une expérience minimales en informatique. La procédure d'installation est automatisée autant que possible.
49.	Le système dispose en permanence d'un environnement d'essai et de validation.
50.	Le coût annuel de maintenance et d'assistance a pu être réduit au minimum grâce au respect des normes du marché et au fait que l'application a été élaborée de façon à ce que seule une assistance minimale, fournie par un service central, soit nécessaire.

3.2.8. Spécifications pour la conception

Nº	Description
51.	Le système est conçu et documenté en prévision d'une durée de fonctionnement de plusieurs années.
52.	Le système a été conçu de façon à ce qu'il soit indépendant du fournisseur de réseau.
53.	Le système est compatible avec le matériel et les logiciels actuellement déployés dans les États membres, puisqu'il interagit avec ces systèmes d'immatriculation grâce à des technologies standard en matière de services web: XML, XSD (XML Schema Definition), SOAP, WSDL (Web Services Description Language), HTTP(s), services web, WS-Security, X.509, etc.

3.2.9. Normes applicables

Nº	Description
54.	Le système est conforme aux dispositions en matière de protection des données prévues par le règlement (CE) nº 45/2001 (articles 21, 22 et 23) et la directive 95/46/CE.
55.	Le système est conforme aux normes IDA.
56.	Le système est compatible avec l'encodage UTF-8.

CHAPITRE 4: **Évaluation**

1. ***Procédure d'évaluation en vertu de l'article 20 (préparation des décisions conformément à l'article 25, paragraphe 2, de la décision 2008/615/JAI)***

1.1. *Questionnaire*

Le groupe de travail concerné du Conseil élaborera un questionnaire concernant chacun des échanges de données automatisés visé au chapitre 2 de la décision 2008/615/JAI.

Lorsqu'un État membre estime qu'il satisfait aux conditions pour l'échange de données appartenant à la catégorie pertinente, il répond au questionnaire adéquat.

1.2. *Essai en conditions réelles*

En vue d'évaluer les résultats du questionnaire, les États membres qui souhaitent commencer à échanger des données effectuent un essai en conditions réelles en collaboration avec un ou plusieurs États membres qui procèdent déjà à de tels échanges en vertu de la décision du Conseil. L'essai a lieu un peu avant ou après la visite d'évaluation.

Les conditions et les modalités de cet essai sont établies par le groupe de travail concerné du Conseil, sur la base d'un accord préalable avec l'État membre concerné. Les États membres qui participent à l'essai en conditions réelles en arrêtent les modalités pratiques.

1.3. *Visite d'évaluation*

En vue d'évaluer les résultats du questionnaire, une visite d'évaluation a lieu dans l'État membre qui souhaite commencer à échanger des données.

Les conditions et les modalités de la visite sont arrêtées par le groupe de travail concerné du Conseil, sur la base d'un accord préalable entre l'État membre concerné et l'équipe d'évaluation. L'État membre concerné donne à l'équipe d'évaluation la possibilité de vérifier l'échange automatisé de données appartenant à la ou aux catégories qui font l'objet de l'évaluation, en particulier en organisant un programme de visite tenant compte des demandes de l'équipe d'évaluation.

L'équipe élabore, dans un délai d'un mois, un rapport concernant la visite d'évaluation et le transmet à l'État membre concerné pour qu'il puisse formuler des observations. Au besoin, l'équipe d'évaluation modifie le rapport en fonction des observations formulées par l'État membre.

L'équipe d'évaluation comprend trois experts au plus; ils sont désigné par les États membres participant à l'échange automatisé des données appartenant aux catégories qui font l'objet de l'évaluation, disposent d'une expérience dans ladite catégorie, ont reçu, au niveau national, l'habilitation de sécurité appropriée pour traiter ces questions et acceptent de participer à au moins une visite d'évaluation dans un autre État membre. La Commission sera invitée à rejoindre l'équipe d'évaluation en tant qu'observateur.

Les membres de l'équipe d'évaluation respecteront le caractère confidentiel des informations qu'ils collectent en s'acquittant de leur mission.

1.4. *Rapport au Conseil*

Un rapport général d'évaluation, comprenant un résumé des résultats des questionnaires, de la visite d'évaluation et de l'essai en conditions réelles, sera présenté au Conseil dans le cadre de la décision qu'il doit prendre en vertu de l'article 25, paragraphe 2, de la décision 2008/615/JAI.

2. ***Procédure d'évaluation conformément à l'article 21***

2.1. *Statistiques et rapport*

Chaque État membre établit des statistiques sur les résultats de l'échange de données automatisé. Pour garantir que ces données soient comparables, le modèle statistique sera mis au point par le groupe de travail concerné du Conseil.

Ces statistiques seront transmises annuellement au secrétariat général, qui élaborera un aperçu pour l'année écoulée, et à la Commission.

En outre, il sera demandé aux États membres, sur une base périodique et pas moins d'une fois par an, de fournir de plus amples informations sur la mise en œuvre administrative, technique et financière de l'échange de données automatisé, aux fins de l'analyse et de l'amélioration du processus. Le Conseil rédigera un rapport sur la base de ces informations.

2.2. *Révision*

Dans un délai raisonnable, le Conseil examinera le mécanisme d'évaluation décrit dans cette partie et le révisera au besoin.

3. Réunion d'experts

Des experts se réuniront périodiquement au sein du groupe de travail concerné du Conseil, afin d'organiser et de mettre en œuvre les procédures d'évaluation visées ci-dessus, de faire part de leur expérience et d'examiner les améliorations possibles. S'il y a lieu, les résultats de ces réunions d'experts figureront dans le rapport visé au point 2.1 ci-dessus.