OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition, 2021

Partie 2 : Spécifications pour la sécurité de la conception, de la fabrication et de la délivrance des DVLM

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition, 2021

Partie 2 : Spécifications pour la sécurité de la conception, de la fabrication et de la délivrance des DVLM

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Publié séparément en français, en anglais, en arabe, en chinois, en espagnol et en russe par l'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
999, boul. Robert-Bourassa, Montréal (Québec) H3C 5H7 Canada

Le site www.icao.int/security/mrtd permet de télécharger les documents et d'obtenir des renseignements supplémentaires.

Doc 9303, *Documents de voyage lisibles à la machine*
Partie 2 — *Spécifications pour la sécurité de la conception, de la fabrication et de la délivrance des DVLM*

Commande nº : 9303P2
ISBN 978-92-9265-492-4 (version imprimée)

AMENDEMENTS

La parution des amendements est annoncée dans les suppléments au *Catalogue des produits et services*. Le Catalogue et ses suppléments sont disponibles sur le site web de l'Organisation (www.icao.int). Le tableau ci-dessous est destiné à rappeler les divers amendements.

RELEVÉ DES AMENDEMENTS ET DES RECTIFICATIFS

AMENDEMENTS		
N°	Date	Inséré par

RECTIFICATIFS		
N°	Date	Inséré par

TABLE DES MATIÈRES

Page

1. PORTÉE

La présente partie contient des spécifications obligatoires et des spécifications optionnelles sur les précautions que doivent prendre les autorités de délivrance de documents de voyage pour sécuriser, contre tout acte frauduleux, les DVLM et les moyens utilisés pour les personnaliser et les délivrer à leurs titulaires légitimes. Elle présente aussi des spécifications obligatoires et des spécifications optionnelles sur la sécurité physique des locaux où les DVLM sont produits, personnalisés et délivrés, ainsi que sur le contrôle de sécurité des personnels chargés de ces opérations.

L'augmentation du nombre de voyageurs dans le monde, la croissance prévue dans ce secteur ainsi que l'accroissement de la criminalité, du terrorisme et de l'immigration illégale sur le plan international suscitent de plus en plus de préoccupations au sujet de la sécurité des documents de voyage et appellent des recommandations sur ce qui peut être fait pour aider à améliorer leur résistance aux violations ou à l'utilisation abusive. Le Doc 9303 n'a fait par le passé aucune recommandation sur les éléments de sécurité spécifiques à incorporer dans les documents de voyage. Les États émetteurs ont eu toute liberté d'incorporer les moyens de protection qu'ils estimaient appropriés pour protéger les documents de voyage qu'ils émettaient contre la contrefaçon, la falsification et d'autres formes de violation, pourvu que ne soit inclus aucun élément susceptible de compromettre la lisibilité par machine de leurs caractères ROC.

Pour répondre à la nécessité d'accroître la sécurité des documents, les conseillers techniques de l'OACI ont jugé souhaitable de publier un ensemble de « normes de sécurité minimales recommandées », qui serviraient de lignes directrices pour tous les États émetteurs de DVLM. En conséquence :

- l'Appendice A fournit des conseils sur le renforcement de la sécurité des documents de voyage lisibles à la machine ;
- l'Appendice B énonce des recommandations relatives à l'authentification par machine des éléments de sécurité dans le document ;
- l'Appendice C décrit les mesures à prendre pour assurer la sécurité des opérations de personnalisation et des documents en transit ;
- l'Appendice D décrit les risques de fraude liés au processus de demande et de délivrance des DVLM.

2. SÉCURISATION DES DVLM ET DE LEUR DÉLIVRANCE

Avant la délivrance d'un document de voyage, l'établissement du titulaire et de son droit à un document de voyage doit être effectué conformément aux [preuves d'identification de l'OACI], *TRIP Guide on Evidence of Identity*, OACI, disponible à l'adresse suivante :https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

Le DVLM et sa méthode de délivrance doivent être conçus de manière à incorporer des moyens de protection du document contre toute attaque frauduleuse durant sa période de validité. Les méthodes d'attaque frauduleuse peuvent être classées comme suit :

- *Contrefaçon.* Il s'agit de la création, intégrale ou partielle, d'un document qui ressemble au DVLM authentique avec l'intention de l'utiliser comme s'il était authentique. Des contrefaçons peuvent être produites en tentant de reproduire ou de simuler la méthode légitime de fabrication et les matériaux qu'elle utilise, ou en ayant recours à des techniques de reprographie.

- *Altération frauduleuse, également appelée falsification*. Il s'agit de la modification d'un document authentique pour en permettre l'utilisation pour des voyages par une personne non autorisée ou vers une destination non autorisée. Les données personnelles du titulaire légitime, en particulier le portrait, constituent la cible principale d'une telle altération.

- *Imposteurs*. Par définition, un « imposteur » est une personne qui se fait passer pour une autre. Des éléments de sécurité devraient être incorporés au DVLM pour faciliter la détection, par les préposés et/ou par machine, de toute utilisation frauduleuse du document par un imposteur.

- *Usurpation.* Fausser l'adresse d'envoi d'une transmission pour s'introduire illégalement dans un système sécurisé.

  Note.— L'usurpation d'identité, la fausse identité, l'accès à califourchon (piggybacking) et le déguisement sont des formes d'usurpation d'identité.

- *Morphose*. La morphose est une technique de manipulation d'images par laquelle les visages de deux ou plusieurs sujets sont morphés ou mélangés pour former un seul visage sur une photographie.

Il existe des méthodes établies de sécurisation pour assurer la protection contre ces types d'attaques frauduleuses. Elles comportent l'utilisation de matériaux qui ne sont pas facilement disponibles, combinée à des systèmes de conception hautement spécialisés et à des procédés de fabrication exigeant de l'expertise et un équipement spécialisé. L'Appendice A à la présente partie recense certaines des techniques actuellement disponibles pour sécuriser les DVLM en permettant à un agent d'inspection de déceler un document contrefait ou altéré frauduleusement, soit à l'œil nu, soit à l'aide de matériel simple tel qu'une loupe ou une lampe à rayonnement ultraviolet.

Tous les DVLM conformes au Doc 9303 doivent utiliser les éléments de sécurité de base indiqués au Tableau A-1 de l'Appendice A.

3. VÉRIFICATION DE DOCUMENTS ASSISTÉE PAR MACHINE

Dans le domaine de l'authentification assistée par machine des documents de voyage lisibles par machine (DVLM), des progrès considérables ont été réalisés au cours de la dernière décennie. Les innovations techniques réalisées dans la conception de la sécurité des DVLM et dans le développement des systèmes d'authentification (lecteurs, logiciels, etc.) ont permis à l'authentification des documents par machine de devenir une partie intégrante de plusieurs infrastructures et processus de contrôle (par exemple, le contrôle aux frontières).

Cependant, de nouveaux défis se posent aux experts en documents, aux fabricants et aux autorités impliquées dans ce domaine, car les améliorations techniques permettent d'accroître la sécurité et l'efficacité des processus opérationnels. Certains des principaux défis sont le manque d'harmonisation et de normalisation des processus en place, et le manque de coordination entre les principales parties participant à ces processus, ce qui entraîne que les parties et les composants du système soient développés indépendamment sans tenir compte des implications majeures résultant de leur interaction. En outre, la complexité et la diversité des systèmes actuellement disponibles sur le marché rendent particulièrement difficile leur évaluation et/ou leur comparaison.

La présente section contient des conseils sur l'authentification assistée par machine des éléments de sécurité incorporés dans les DVLM et conformes aux spécifications du Doc 9303. L'Appendice A à la présente partie et les normes de sécurité qui y sont recommandées ; constituent la base des considérations de la présente section. L'Appendice B énonce des recommandations qui couvrent la vérification par machine de ces normes de sécurité (basées sur les matériaux, sur l'impression de sécurité et sur les techniques de protection contre la copie) en utilisant la capacité des lecteurs de documents à acquérir des images à haute résolution dans la gamme spectrale visuelle

infrarouge et ultraviolette. Enfin, l'Appendice C fournit un ensemble de recommandations de meilleures pratiques pour les principales parties participant à la conception, à la mise en œuvre et au fonctionnement des systèmes d'authentification des machines et de leurs éléments clés.

Le succès mondial de l'initiative de l'OACI en matière de documents électroniques s'est traduit par la délivrance de millions de DVLM-e conformes aux spécifications du Doc 9303. Les concepts avancés appliqués à ces documents requièrent l'emploi d'appareils de lecture de documents de voyage capables de lire les circuits imprimés (CI) sans contact aux points d'authentification des documents, qui sont habituellement les points d'entrée à une frontière d'un pays. Ces lecteurs évolués permettent non seulement de lire les CI sans contact, mais aussi d'acquérir des images haute résolution dans la région visuelle, infrarouge et ultraviolette du spectre.

Les recommandations de la présente section ont pour but d'améliorer la sécurité des documents de voyage lisibles à la machine dans le monde entier en utilisant des procédures de vérification des documents assistée par machine :

- qui sont conformes à la disposition des DVLM spécifiée dans le Doc 9303 et qui assurent la compatibilité amont ;
- qui sont conformes aux éléments de sécurité recommandés dans l'Appendice A à la présente partie ;
- qui tirent parti des capacités techniques des appareils de lecture évolués installés dans le monde pour prendre en charge les DVLM-e, comme recommandé dans les Appendices B et C de la présente partie.

Cependant, chaque État doit évaluer les risques des éléments d'authentification des documents assistée par machine à ses frontières pour déterminer les caractéristiques les plus avantageuses et réduire les risques au minimum. Le Doc 9303 ne spécifie aucun élément particulier comme moyen de vérification de documents assistée par machine à interopérabilité mondiale car l'emploi universel d'un élément unique rendrait celui-ci extrêmement vulnérable aux attaques frauduleuses. Pour réduire les risques au minimum, les États devraient donc utiliser plusieurs éléments de sécurité.

3.1 Types d'éléments de sécurité

Il y a trois grandes catégories d'éléments de sécurité vérifiables par machine. Elles sont décrites dans les paragraphes qui suivent, avec des exemples d'éléments de sécurité vérifiables par machine.

3.1.1 Éléments de structure

Un élément de structure est une structure mesurable incorporée dans ou sur la page de renseignements d'un DVLM. Il s'agit d'un élément de sécurité contenant un certain type d'information vérifiable reposant sur la construction physique de cet élément. En voici quelques exemples :

- la caractéristique d'interférence d'un hologramme ou de tout autre dispositif optiquement variable qui peut être identifiée de façon unique par un appareil de lecture approprié ;
- des images rétroréfléchissantes intégrées dans un film de sécurité ;
- la transmission contrôlée de la lumière à travers des espaces déterminés du support.

3.1.2 Éléments de substance

Un élément de substance est un matériau incorporé dans un DVLM, qui ne serait pas normalement présent dans le DVLM et dont la présence n'apparaît pas de façon évidente à l'inspection visuelle. La présence de ce matériau peut être détectée par la présence et l'ampleur d'une propriété appropriée de la substance ajoutée. Il s'agit d'identifier une caractéristique définie d'une substance utilisée dans la construction de l'élément. Par exemple :

- utilisation de pigments, généralement dans les encres, qui réagissent d'une façon spécifique et inhabituelle à certaines longueurs d'ondes de la lumière (pouvant inclure l'infrarouge ou l'ultraviolet) ou qui ont des propriétés magnétiques ou électromagnétiques ;

- incorporation, dans un élément de la page de renseignements, de matériaux tels que des fibres, dont la taille ou la répartition par dimensions est conforme à une spécification prédéterminée.

3.1.3 Éléments de données

L'image visible de la page de renseignements d'un DVLM peut contenir des informations cachées, détectables par un dispositif approprié intégré à l'appareil de lecture. Les informations cachées peuvent être dissimulées dans la page de renseignements imprimée de façon sécurisée, mais elles sont le plus souvent incorporées dans les données de personnalisation, notamment le portrait imprimé.

L'insertion d'informations cachées dans la page de renseignements du DVLM peut nécessiter l'application d'éléments de substance et/ou de structure de manière à obtenir plusieurs niveaux de sécurisation. Dans ce contexte, le terme stéganographie décrit une classe particulière d'éléments de données, généralement des informations numériques dissimulées dans une image, habituellement le portrait utilisé pour la personnalisation ou l'impression de sécurité du fond. L'information peut être décodée par un dispositif approprié intégré à un appareil de lecture pleine page, réglé pour rechercher l'élément à un endroit précis. L'information peut, par exemple, être le numéro du document de voyage. L'appareil de lecture pourrait alors être programmé pour comparer le numéro de document de voyage obtenu à partir de l'élément avec le numéro de document de voyage figurant dans la zone de lecture automatique (ZLA). Cette comparaison n'exige pas l'accès à des données stockées sur le CI sans contact d'un DVLM-e. Exemples de ce type d'élément :

- données codées stockées dans le document sur des supports magnétiques tels que des fils de sécurité spéciaux ;

- motifs incorporant les données dissimulées qui ne deviennent détectables que lorsqu'ils sont observés sous une lumière d'une longueur d'onde spécifique ou en utilisant des filtres optiques ou un logiciel de traitement d'image particulier.

Dans des formes plus complexes, le volume de données stockées peut être important, ce qui peut être vérifié par comparaison électronique avec les données stockées dans le CI sans contact du DVLM-e.

3.2 Principes de base

Les trois types d'éléments (structure, substance et données) peuvent être incorporés dans des documents de voyage et vérifiés à l'aide d'appareils de lecture appropriés. Il existe maintenant des lecteurs capables de détecter de tels éléments et d'utiliser les réponses pour confirmer l'authenticité du document. L'Appendice B porte principalement sur des éléments vérifiables par un équipement de détection incorporé dans l'appareil de lecture des DVLM et utilisé pendant le processus de lecture normal

.

La vérification de sécurité des documents assistée par machine utilise une technologie d'inspection automatisée pour aider à vérifier l'authenticité d'un document de voyage. Elle ne devrait pas être employée seule pour établir l'authenticité d'un document mais, utilisée en combinaison avec les éléments de sécurité visibles du document, elle offre à l'examinateur un nouvel outil puissant d'aide à la vérification des documents de voyage.

Les éléments de vérification de sécurité des documents assistée par machine sont des éléments de sécurité optionnels qui peuvent être inclus dans le DVLM à la discrétion de l'autorité de délivrance.

La taille des éléments de sécurité vérifiables par machine peut varier entre moins d'un millimètre (0,04 in) carré et la superficie totale du document. La Figure 1 donne des indications sur les positions que ces éléments devraient occuper sur la page de renseignements d'un DVLM pour faciliter l'interopérabilité. Il est recommandé, pour assurer la compatibilité amont, de placer les éléments d'authentification par machine dans les positions et les zones indiquées.

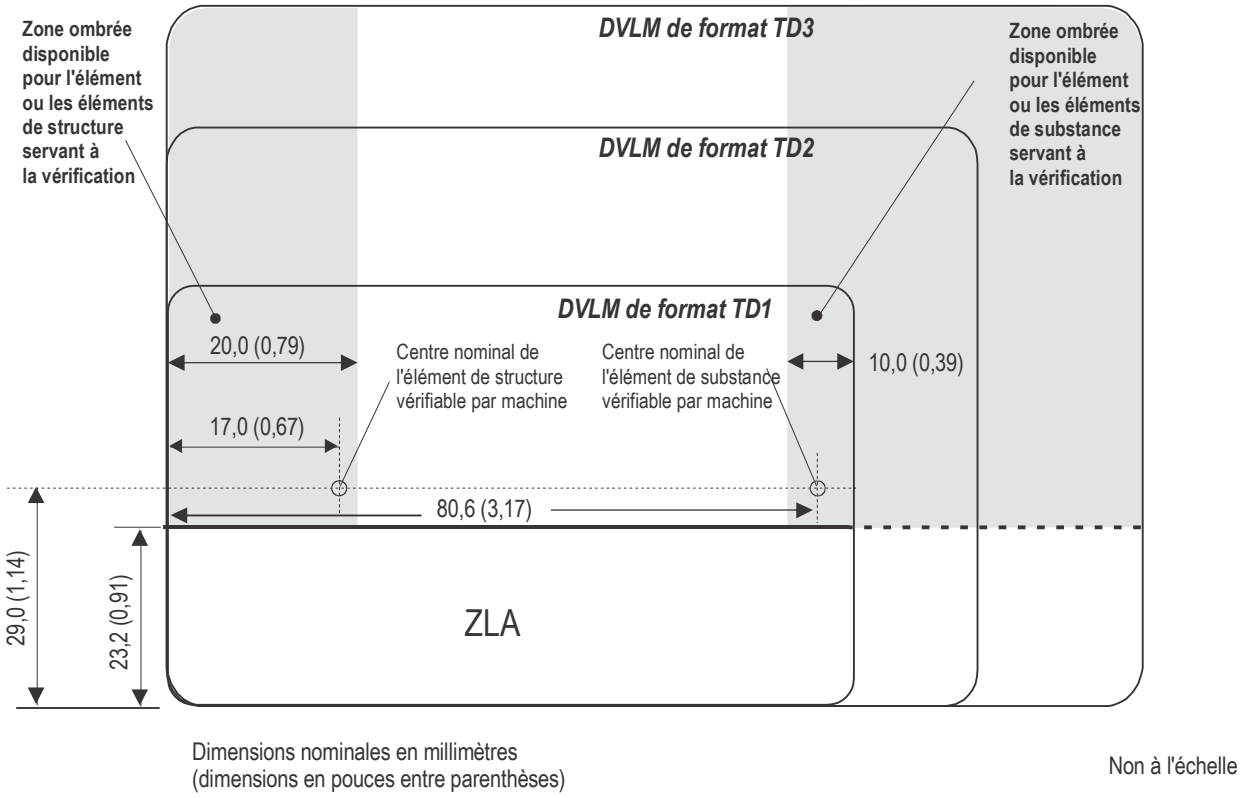

Figure 1. Trois formats de DVLM, y compris le PLM (format TD3), avec les positions recommandées pour les éléments servant à la vérification de document assistée par machine. Il est recommandé d'utiliser la zone ombrée de gauche pour l'incorporation d'un élément de structure et celle de droite pour l'incorporation d'un élément de substance.

3.3 Authentification par machine et DVLM-e

L'emploi, dans un DVLM-e, d'un CI sans contact entièrement conforme offre d'excellentes possibilités d'authentification par machine. Cependant, l'authentification par machine avec un CI sans contact échoue :

- si le CI sans contact est défectueux et ne communique pas ; ou
- si aucun certificat n'est disponible pour vérifier l'authenticité et l'intégrité des données contenues dans le CI sans contact.

Il est donc nécessaire d'avoir un autre moyen d'authentification par machine, surtout dans le cas des contrôles frontaliers automatisés (CFA) où la lecture et la validation des DVLM-e sont effectuées par des lecteurs de documents plutôt que par un agent des services frontaliers. Comme autre moyen fiable, l'authentification par lecteur optique établit la confiance dans les données utilisées pour prendre les décisions aux frontières.

Un CI sans contact qui fonctionne correctement dans un DVLM-e peut aussi faciliter l'authentification par lecteur optique en stockant des éléments d'authentification par lecture optique et ses coordonnées dans les groupes de données (DG) pertinents.

4. SÉCURISATION DES INSTALLATIONS DE PRODUCTION (CONCEPTION ET FABRICATION) ET DE DÉLIVRANCE DES DVLM

L'État qui émet un DVLM doit veiller à ce que les locaux dans lesquels le DVLM est imprimé, relié, personnalisé et délivré soient convenablement sécurisés et à ce que le personnel qui y est employé possède une habilitation de sécurité appropriée. La sécurité des DVLM doit aussi être convenablement assurée durant le transport entre les différents locaux et entre les installations de production et le lieu de délivrance du DVLM au titulaire. L'Appendice C donne des recommandations sur la manière de satisfaire à ces exigences.

Il convient de tenir compte des facteurs suivants dans l'établissement des installations de production et de délivrance des DVLM :

1) résilience ;
2) sécurité physique et contrôle d'accès ;
3) matériels de production et comptabilité des DVLM ;
4) transport ;
5) personnel ;
6) cybersécurité.

4.1 Résilience

Les États doivent prendre les mesures nécessaires pour poursuivre la production des DVLM en cas de catastrophes telles qu'une inondation, un incendie ou une défaillance de l'équipement. Ces mesures peuvent comprendre notamment :

- des installations de production et de délivrance décentralisées ;

- des installations de production secondaires lorsque la production est centralisée ;
- des installations de délivrance d'urgence ;
- un accès rapide aux pièces de rechange et au soutien ;
- une deuxième source d'approvisionnement de tous les composants des DVLM.

Il est recommandé aux États de tenir compte des modes de défaillance possibles dans la conception des installations de production et de délivrance des DVLM afin d'éliminer les défaillances communes et les points uniques de défaillance.

4.2 Sécurité physique et contrôle d'accès

Les États doivent contrôler l'accès aux installations de production et de délivrance. Le contrôle devrait être effectué par zones et les critères d'accès à chaque zone devraient être proportionnels à la valeur des éléments protégés.

Voici quelques exemples de bonnes pratiques à appliquer aux installations de production :

- zones de production séparées par des treillis métalliques ou des murs pleins ;
- chambres fortes pour conserver les DVLM finis non personnalisés et les éléments de sécurité clés pour la production des DVLM ;
- contrôle d'accès entre les zones au moyen d'un laissez-passer ;
- vidéosurveillance à l'intérieur et à l'extérieur de l'installation ;
- sécurité du périmètre ;
- personnel de sûreté à plein temps.

Les États devraient aussi tenir compte de la sécurité assurée dans les organismes qui fournissent les composants de DVLM à l'installation de production, car le vol ou la vente de ces composants peut faciliter la falsification des DVLM.

Les zones des services administratifs et les zones publiques des installations où sont délivrés les DVLM devraient être séparées et l'accès entre les deux devrait être contrôlé. Le personnel doit être convenablement protégé et la protection doit être déterminée en fonction des circonstances locales.

4.3 Comptabilité du matériel de production

Les États doivent veiller à ce que tout le matériel utilisé dans la production des DVLM soit compté et à ce que la production des DVLM concorde avec les commandes de DVLM, de manière à confirmer qu'il ne manque aucun DVLM ni aucun composant de DVLM.

Le matériel, les DVLM et les composants de DVLM défectueux doivent être détruits de manière sûre et comptés pour s'assurer que rien ne manque.

En général, la comptabilité du matériel est plus facile lorsque le nombre de lieux de production et de délivrance est moindre, mais il faut aussi tenir compte de la nécessité d'assurer la résilience et un service acceptable à la clientèle.

4.4 Transport

Il est conseillé aux États d'employer des méthodes sûres pour transporter les DVLM et les composants de DVLM ; les méthodes de transport de fonds sont habituellement suffisantes à moins de transporter des éléments de très grande valeur (par exemple, les matrices holographiques).

Les États devraient s'efforcer de réduire au minimum la quantité de matériel transporté dans un lot afin de réduire les incidences d'un vol. En particulier, les États ne devraient pas transporter des ensembles complets de plaques d'impression en un seul déplacement.

4.5 Personnel

Les États doivent veiller à ce que tous les membres du personnel soient soumis à un processus d'habilitation de sécurité pour confirmer leur identité et leur aptitude à travailler dans un environnement où sont fabriqués des produits de grande valeur. Il faut fournir aux membres du personnel les justificatifs d'identité nécessaires pour leur permettre d'entrer dans les zones auxquelles ils doivent avoir accès pour exercer leurs fonctions.

4.6 Cybersécurité

Les installations de production et de délivrance sont vulnérables aux cyberattaques, par exemple :

1) virus et autres maliciels, tant dans les installations informatiques traditionnelles que dans l'équipement de production ;

2) attaques par déni de service par le biais des canaux de demande de DVLM en ligne et des services web utilisés par les systèmes de production et de délivrance ;

3) compromission des systèmes d'émission, permettant aux attaquants d'émettre et de délivrer des passeports ou de voler des données personnelles ou des éléments cryptographiques (comme les clés privées pour la production des DVLM-e).

Les mesures à prendre pour contrer ces attaques ou autres attaques similaires dépassent le cadre du présent document. Il est recommandé aux États de demander l'avis de leurs autorités techniques nationales respectives.

5. COMMUNICATION DE RENSEIGNEMENTS SUR LES DVLM NOUVELLEMENT ÉMIS

Il est recommandé qu'un État qui lance un nouveau modèle de DVLM communique à tous les autres États des renseignements détaillés sur ce nouveau DVLM, y compris les éléments de sécurité évidents, de préférence en fournissant des spécimens personnalisés que le service de l'État récepteur chargé de vérifier l'authenticité de ces documents utilisera comme référence. Ces spécimens devraient être remis à des points de contact établis, convenus par les États récepteurs.

6. COMMUNICATION DE RENSEIGNEMENTS SUR LES DVLM PERDUS OU VOLÉS

L'échange de renseignements sur les documents de voyage perdus, volés ou révoqués est une stratégie essentielle pour renforcer les contrôles frontaliers et réduire les incidences des vols d'identité et la fraude en matière d'immigration. Les États devraient donc envisager de mettre en œuvre les procédures opérationnelles suivantes pour neutraliser les menaces qui visent à compromettre la gestion des frontières et la sécurité nationale :

1. communication proactive avec les titulaires de documents ;
2. tenue de bases de données nationales des documents de voyage perdus, volés ou révoqués ;
3. partage de renseignements sur les documents de voyage perdus, volés ou révoqués avec INTERPOL et vérification systématique des documents dans les bases de données d'INTERPOL lors de l'inspection primaire ;
4. mise en place de contrôles pour déterminer si une personne qui se présente à un point de passage d'une frontière détient un document perdu, volé ou révoqué.

6.1 Communication proactive avec les titulaires de documents

Les États doivent veiller à ce que les titulaires de documents de voyage soient pleinement conscients de leurs responsabilités en ce qui concerne l'utilisation et la protection de leurs documents de voyage, et des procédures de déclaration de perte ou de vol de ces documents. Des directives sur la protection des documents de voyage à la maison et pendant les voyages peuvent aider à en prévenir la perte ou le vol. Lorsqu'ils reçoivent leurs documents de voyage, les titulaires des documents doivent être informés des mesures et des moyens à prendre pour déclarer la perte ou le vol de leurs documents (notamment la nécessité de le déclarer rapidement). Pour faciliter le processus, les États pourraient envisager de mettre à leur disposition plusieurs moyens (en personne, par téléphone, par courrier et par d'autres moyens de communication électroniques, notamment Internet) pour leur permettre de signaler la perte ou le vol de leurs documents.

Les États doivent aussi prendre les mesures appropriées pour veiller à ce que les titulaires de documents de voyage soient conscients des perturbations, des inconvénients et des dépenses supplémentaires qu'ils pourraient subir lorsque des documents perdus, volés ou révoqués sont présentés aux contrôles frontaliers à des fins de voyage. Les renseignements qui leur sont fournis devraient souligner le fait qu'une fois qu'un document est déclaré perdu ou volé, il est annulé et ne peut plus être utilisé, et qu'il peut être saisi par les autorités s'il y a tentative de s'en servir.

Il convient de mettre en place une législation nationale, ou tout autre cadre approprié, pour obliger les titulaires de documents de voyage à déclarer immédiatement la perte ou le vol d'un document de voyage. Aucun nouveau document de voyage ne devrait être délivré avant que cette perte ou ce vol n'aient été signalés.

6.2 Tenue de bases de données nationales des documents de voyage perdus, volés ou révoqués

Les États qui utilisent des bases de données nationales de documents de voyage pour faciliter la vérification du statut des documents de voyage qu'ils émettent doivent faire en sorte que les informations soient tenues à jour. Les déclarations de documents perdus ou volés faites par les titulaires des documents doivent être rapidement consignées dans ces systèmes afin d'assurer l'exactitude des évaluations de risques effectuées sur la base de ces systèmes. Les États pourraient aussi envisager d'inclure dans ces bases de données des renseignements sur les documents perdus, volés ou révoqués qui ont été interceptés. En plus d'actualiser les bases de données, les États doivent s'assurer que les autorités de contrôle frontalier et les autorités policières peuvent facilement y accéder.

6.3 Partage de renseignements sur les documents de voyage perdus, volés ou révoqués avec INTERPOL et vérification systématique des documents dans les bases de données d'INTERPOL lors de l'inspection primaire

Les États devraient participer à l'échange mondial de renseignements opportuns et précis sur le statut des documents de voyage pour faciliter les contrôles nationaux et la gestion des frontières, et contribuer aux efforts déployés pour réduire les incidences des vols d'identité. L'échange de renseignements sur les documents de voyage perdus, volés ou révoqués permet :

a) d'améliorer l'intégrité de la gestion des frontières ;

b) de faciliter la détection des vols d'identité ou de la fraude en matière d'immigration aux frontières ou dans d'autres situations où les documents sont présentés comme moyen d'identification ;

c) d'augmenter les chances d'identifier les agents terroristes voyageant avec de faux documents ;

d) d'augmenter les chances d'identifier les activités criminelles, notamment le trafic de migrants ;

e) d'aider à récupérer des documents nationaux ;

f) de limiter la valeur et l'utilisation des documents perdus, volés ou révoqués pour les activités illégales.

Le système de recherche automatique — base de données sur les documents de voyage perdus ou volés (ASF-SLTD) d'INTERPOL permet aux États de communiquer rapidement et efficacement des renseignements sur les documents de voyage perdus, volés ou révoqués. Ces renseignements devraient porter sur les documents délivrés qui ont été perdus ou volés ainsi que sur les documents vierges qui ont été volés dans une installation de production, un point de délivrance ou pendant le transport. L'Appendice D précise les facteurs à prendre en compte avant de participer à l'ASF-SLTD.

Les États devraient systématiquement vérifier les documents par rapport aux informations des bases de données d'INTERPOL au moment de l'inspection primaire afin de s'assurer que seuls les voyageurs qui détiennent des documents de voyage valides franchissent les points de contrôle frontalier. La vérification du statut des documents de voyage par rapport aux informations de ces bases de données offre un grand nombre des mêmes avantages que l'échange de renseignements sur les documents perdus, volés ou révoqués.

6.4 Mise en place de contrôles pour déterminer si une personne qui se présente à un point de passage d'une frontière détient un document perdu, volé ou révoqué

Les États doivent travailler dans le cadre de leurs législations nationales et respecter les accords internationaux sur l'utilisation des documents de voyage et les contrôles frontaliers dans le traitement des voyageurs qui se présentent à leurs frontières. Tous les voyageurs qui détiennent des documents de voyage déclarés perdus, volés ou révoqués doivent être traités comme s'il n'existait aucune intention illégale, jusqu'à preuve du contraire.

6.4.1 Documents de voyage figurant dans les documents perdus, volés ou révoqués de la base de données d'INTERPOL

L'entrée ou la sortie d'un voyageur ne devrait pas être refusée simplement parce que le document figure dans la base de données des documents de voyage perdus, volés ou révoqués. Les États doivent prendre plusieurs mesures pour étayer ce refus. Si un voyageur détient un document de voyage qui est enregistré comme perdu, volé ou révoqué dans l'ASF-SLTD, les États doivent, dans la mesure du possible, communiquer avec le pays qui a émis le document et l'a consigné dans la base de données pour confirmer que le document a été correctement enregistré comme perdu, volé

ou révoqué. Les États doivent aussi avoir une entrevue avec les voyageurs pour vérifier leur identité ou leur nationalité et déterminer s'ils sont vraiment les titulaires légitimes des documents de voyage.

Si le document contient une puce, les États devraient procéder à des vérifications biométriques pour essayer de déterminer la véritable identité du voyageur. Ils devraient aussi essayer de déterminer si les données ont été altérées et si le document est authentique.

6.4.2 Traitement du titulaire légitime du document de voyage au point de contrôle frontalier

Lorsqu'ils traitent avec les titulaires légitimes de documents de voyage, les États devraient être conscients du fait que la personne identifiée comme le titulaire légitime d'un document de voyage déclaré perdu, volé ou révoqué ne tente pas nécessairement de commettre une infraction pénale. Au lieu d'essayer de punir ces personnes, les États devraient plutôt s'efforcer de trouver des moyens de retirer ces documents de la circulation, tout en perturbant le moins possible les déplacements. Lorsque la législation nationale le permet, les États pourraient envisager d'appliquer à ces voyageurs des procédures différentes de celles qui sont appliquées aux personnes qui tentent intentionnellement d'entrer illégalement dans le pays en usurpant une identité.

Voyageurs entrant dans un pays étranger avec un document déclaré perdu, volé ou révoqué par suite d'une erreur de données	Le poste de contrôle frontalier de l'État récepteur devrait communiquer avec l'autorité de délivrance pour confirmer qu'il s'agit bien d'une erreur de données. Une fois l'erreur confirmée, les États peuvent traiter le document comme un document de voyage valide, mais devraient recommander au voyageur de communiquer avec l'autorité de délivrance dès son retour dans son pays. Les autorités de délivrance de documents de voyage de l'État émetteur doivent prendre toutes les mesures nécessaires pour supprimer ce document de la base de données des documents perdus, volés ou révoqués. Les États doivent aussi envisager de remplacer le document en cause sans frais pour le titulaire.
Ressortissants essayant de quitter leur pays avec un document déclaré perdu ou volé	Lorsqu'il existe des contrôles de sortie, le poste de contrôle frontalier devrait indiquer à ces voyageurs que leurs documents ne sont pas valides et qu'ils doivent obtenir un document de voyage valide avant d'entreprendre leur voyage vu que les documents perdus, volés ou révoqués ne sont pas considérés comme valides.
Ressortissants essayant de quitter leur pays avec un document révoqué	Lorsqu'il existe des contrôles de sortie, le poste de contrôle frontalier devrait consulter les services policiers nationaux pour déterminer les mesures ou lois qui peuvent être invoquées pour empêcher la personne de quitter le pays. Si ces mesures ou lois l'autorisent, les autorités de gestion des frontières ou les services de police aux frontières devraient empêcher ces voyageurs de quitter l'État.
Ressortissants essayant de quitter un pays et de retourner dans leur pays avec un document déclaré perdu, volé ou révoqué	Lorsqu'il existe des contrôles de sortie et que l'identité et la nationalité du détenteur ont été confirmées, le poste de contrôle frontalier peut permettre aux voyageurs de partir, mais il devrait les informer que le document qu'ils ont présenté n'est pas valide et que le transporteur peut leur refuser l'embarquement.

	Lorsque des voyageurs reviennent dans leur pays d'origine avec un document déclaré perdu, volé ou révoqué, le poste de contrôle frontalier peut, lorsque la législation nationale ou un accord international le lui permet, saisir ou confisquer le document pour le renvoyer à l'émetteur. Il convient de recommander aux voyageurs dont les documents ont été saisis ou confisqués d'obtenir de nouveaux documents de voyage valides.
Ressortissants essayant de quitter un pays étranger et de continuer vers un troisième pays avec un document déclaré perdu, volé ou révoqué	Lorsqu'il existe des contrôles de sortie, le poste de contrôle frontalier devrait indiquer aux voyageurs que leurs documents de voyage ne sont pas valides, que le transporteur peut leur refuser l'embarquement et qu'ils peuvent avoir des difficultés à leur arrivée à leur prochaine destination.
Voyageurs entrant dans un pays étranger avec un document perdu, volé ou révoqué	L'État récepteur devrait indiquer aux voyageurs qui ont eu l'autorisation d'embarquement de communiquer avec leur consulat ou leur ambassade afin d'obtenir un document de voyage valide avant d'essayer de poursuivre leur voyage. Les voyageurs auxquels l'entrée a été refusée peuvent être traités conformément à la législation nationale.

6.4.3 Traitement des voyageurs après avoir déterminé qu'ils ne sont pas les titulaires légitimes d'un document déclaré perdu, volé ou révoqué

Lorsqu'il est établi qu'un voyageur n'est pas le titulaire légitime d'un document de voyage, les autorités frontalières ou policières de l'État émetteur ou de l'État récepteur doivent s'efforcer de déterminer comment le voyageur a pris possession du document, notamment s'il y a eu collusion avec le titulaire légitime du document et, si la législation nationale le permet et en travaillant en coopération avec l'État émetteur, déterminer si d'autres documents frauduleux portant cette identité ont été délivrés. S'il est établi que le voyageur a présenté un document de voyage perdu, volé ou révoqué, les États doivent enquêter sur le voyageur et, s'il y a lieu, engager des poursuites pénales et/ou lui faire quitter leur État.

Les États devraient confisquer les documents pour les utiliser dans les procédures judiciaires, notamment les procédures de traitement des dossiers d'immigrants et de réfugiés, mais ils doivent retourner ces documents à l'État émetteur lorsqu'ils ne sont plus nécessaires. Il convient également, si la législation nationale le permet, de communiquer le plus de renseignements possible sur l'interception à l'émetteur.

Les États devraient aussi s'assurer que les personnes qui ne sont pas admissibles sont munies de documents conformes à l'Annexe 9 — *Facilitation* à la Convention relative à l'aviation civile internationale.

7. RÉFÉRENCES (NORMATIVES)

Certaines dispositions des normes internationales constituent, par référence, des dispositions du Doc 9303. En cas de différences entre les spécifications du Doc 9303 et les normes citées en référence, pour tenir compte des besoins spécifiques de la réalisation de documents de voyage lisibles par machine, y compris les visas lisibles par machine, les spécifications énoncées dans le présent document prévalent.

Annexe 9 à la Convention relative à l'aviation civile internationale (« Convention de Chicago »), Annexe 9 – *Facilitation.*

[Preuves d'identification de l'OACI] *TRIP Guide on Evidence of Identity*, OACI, disponible à l'adresse suivante : https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

— — — — — — — —

APPENDICE A À LA PARTIE 2
(INFORMATIF)

NORMES DE SÉCURITÉ DES DVLM

A.1 PORTÉE

Le présent appendice donne des orientations sur le renforcement de la sécurité des DVLM établis conformément aux spécifications du Doc 9303. Les recommandations portent sur la sécurité des matériaux utilisés dans la construction du document, les techniques d'impression de sécurité et de protection contre la copie à employer et les procédés à utiliser dans la production des documents vierges. Les considérations de sécurité qui s'appliquent à la personnalisation et à la protection des données personnelles figurant dans le document sont aussi abordées. Toutes les autorités qui émettent des documents de voyage doivent tenir compte du présent appendice.

A.2 INTRODUCTION

Le présent appendice identifie les menaces auxquelles les documents de voyage sont fréquemment exposés et les parades qui peuvent être employées pour protéger ces documents et les systèmes de personnalisation connexes. Les listes d'éléments et/ou de techniques de sécurisation qui offrent une protection contre les menaces ont été subdivisées en : 1) éléments et/ou techniques de sécurité de base, jugés indispensables, et 2) éléments et/ou techniques supplémentaires, parmi lesquels les États sont encouragés à choisir des éléments qui sont recommandés pour renforcer le niveau de sécurité.

Il est tenu compte du fait qu'un élément ou une technique qui peut être nécessaire pour protéger les documents d'un État peut être superflu ou avoir une importance mineure pour un autre État qui utilise des systèmes de production différents. Une démarche ciblée, qui laisse aux États la possibilité de choisir entre différents systèmes de documents (documents sur support papier, cartes en plastique, etc.) et une combinaison des éléments et/ou des techniques de sécurité les mieux adaptés à leurs besoins particuliers, est donc préférable à une approche uniformisée imposant un modèle unique. Cependant, pour qu'il puisse choisir un ensemble équilibré d'éléments et/ou de techniques de sécurité, chaque État doit procéder à une évaluation des risques auxquels sont exposés ses documents de voyage nationaux, afin d'en identifier les aspects les plus vulnérables et de sélectionner les éléments et/ou les techniques supplémentaires qui apporteront la meilleure solution à leurs problèmes spécifiques.

Le but des recommandations du présent appendice est d'améliorer la sécurité des DVLM dans le monde entier, en établissant des pratiques de référence pour les États émetteurs. Rien dans ces recommandations ne doit empêcher ou dissuader les États de mettre en œuvre, à leur discrétion, d'autres éléments de sécurité plus avancés, afin d'obtenir un niveau de sécurité supérieur à celui que permettent d'assurer les éléments et techniques minimaux recommandés dans le présent appendice.

Cet appendice contient aussi un tableau récapitulatif des divers types de menaces auxquelles sont exposés les documents de voyage et de certains des éléments et techniques de sécurité qui peuvent aider à les protéger contre ces menaces.

A.3 PRINCIPES DE BASE

La production et l'entreposage des passeports en livret et des documents de voyage, y compris les processus de personnalisation, devraient être réalisés dans un environnement sûr et contrôlé, où sont appliquées des mesures de sécurité appropriées pour protéger les locaux contre tout accès non autorisé. Si le processus de personnalisation est décentralisé ou si la personnalisation est réalisée en un lieu séparé géographiquement de celui où les documents de voyage vierges sont confectionnés, il convient de prendre des précautions appropriées pour assurer la sécurité des documents vierges et de tous les matériaux de sécurité connexes pendant leur transport et leur entreposage à l'arrivée. Les passeports en livret et autres documents de voyage vierges en transit devraient contenir le numéro de document unique. Dans le cas des passeports, le numéro de passeport doit figurer sur toutes les pages autres que la page des données personnelles sur laquelle le numéro peut être imprimé lors du processus de personnalisation.

Tout le processus devrait s'accompagner d'une obligation de rendre complètement compte de tous les matériaux de sécurité utilisés dans la production des documents de voyage, y compris ceux qui ont été abîmés, et de faire un rapprochement complet, à chaque étape du processus de fabrication, avec des registres permettant de retracer l'utilisation de tous les matériaux de sécurité. La piste de vérification devrait être suffisamment détaillée pour suivre l'utilisation de chaque unité de matériau de sécurité utilisé dans la production, et la vérification devrait être effectuée de façon indépendante par des personnes n'intervenant pas directement dans la production. Il convient aussi de tenir des registres certifiés à un niveau de supervision de manière à rendre compte de la destruction de tous les matériaux de sécurité et de tous les documents endommagés ou abîmés.

Les matériaux employés dans la production des documents de voyage devraient être de variétés contrôlées, s'il y a lieu, et obtenus uniquement auprès de fournisseurs reconnus de matériaux de sécurité. Il convient d'utiliser des matériaux destinés exclusivement à des applications de haute sécurité et d'éviter l'emploi de matériaux disponibles sur le marché libre.

Il faut éviter de dépendre totalement de logiciels de conception graphique en vente libre pour créer les fonds de sécurité, mais ces logiciels peuvent être employés conjointement avec des logiciels de conception de sécurité spécialisés.

Il convient d'incorporer dans les documents de voyage des éléments et/ou des techniques de sécurité destinés à les protéger contre la reproduction, l'altération et autres manœuvres abusives non autorisées, notamment l'enlèvement et la substitution de pages du passeport en livret, en particulier la page de données personnelles. Il faut, en plus d'incorporer des éléments de protection des documents vierges contre la contrefaçon et la falsification, porter une attention particulière à la protection des données personnelles contre l'enlèvement ou l'altération. Un document de voyage devrait comprendre des éléments et/ou des techniques de sécurité adéquats qui mettent en évidence toute tentative d'altération.

La combinaison d'éléments, de matériaux et de techniques de sécurité devrait être bien choisie afin d'assurer pleinement la compatibilité et la protection du document pendant toute sa durée de vie.

Le présent appendice traite principalement des éléments de sécurité qui aident à protéger les documents de voyage contre la contrefaçon et l'altération frauduleuse, mais il en existe une autre catégorie d'éléments de sécurité (éléments de niveau 3), qui comprend des éléments dissimulés (secrets), destinés à être authentifiés soit par une expertise judiciaire, soit par un matériel de vérification spécialisé. Il est évident que la connaissance de la substance et de la structure précises de ces éléments doit être limitée à un très petit nombre de personnes ayant « besoin d'en connaître ». Ces éléments ont notamment pour but de permettre l'authentification des documents lorsqu'une preuve d'authenticité sans équivoque est impérative (devant un tribunal, par exemple). Tous les documents de voyage devraient contenir en tant qu'élément essentiel au moins un élément de sécurité dissimulé.

L'Annexe 9 — *Facilitation* de l'OACI contient des normes et pratiques recommandées générales importantes sur la période de validité du passeport, le principe du passeport unipersonnel, les échéances pour l'émission de passeports lisibles à la machine (PLM) et le retrait de la circulation de passeports non lisibles par machine, et d'autres indications.

Le seul support de stockage de données acceptable pour l'interopérabilité mondiale est un CI sans contact, qui est spécifié par l'OACI comme la technologie d'expansion de capacité à utiliser pour les DVLM.

A.4 PRINCIPALES MENACES À LA SÉCURITÉ DES DOCUMENTS DE VOYAGE

Les menaces ci-après contre la sécurité des documents, présentées sans ordre d'importance particulier, correspondent à des actes frauduleux dont les documents, leur émission et leur utilisation peuvent faire l'objet :

- contrefaçon d'un document de voyage complet ;
- substitution de photographie ;
- effacement/altération de données dans la zone d'inspection visuelle (ZIV) ou la ZLA de la page de renseignements du PLM ;
- construction, en totalité ou en partie, d'un document frauduleux au moyen de matériaux provenant de documents légitimes ;
- enlèvement et substitution d'une ou de plusieurs pages entières ou de visas ;
- suppression d'indications sur les pages de visas ou la page d'observations ;
- vol de documents vierges authentiques ;
- imposteurs (identité empruntée, apparence modifiée) ;
- altération physique ou électronique du CI sans contact (lorsqu'il est présent).

Les éléments de sécurité peuvent être détectés à l'un quelconque des trois niveaux d'inspection suivants :

- niveau 1 — examen superficiel pour une inspection rapide au point d'utilisation (éléments visuels ou tactiles facilement identifiables) ;
- niveau 2 — examen au moyen d'un équipement simple par des inspecteurs qualifiés ;
- niveau 3 — inspection par des spécialistes de la police scientifique.

Il convient de réexaminer périodiquement la conception du document et d'y apporter les modifications nécessaires pour maintenir la sécurité et l'intégrité du document. Il sera ainsi possible d'incorporer de nouvelles mesures de sécurité dans le document et de certifier sa capacité de résister aux tentatives de compromission ou de fraude en ce qui concerne les points suivants :

- substitution de photographie ;
- délaminage et autres effets de déconstruction ;
- ingénierie inverse du CI sans contact ainsi que d'autres composants ;
- modification d'un élément de données ;
- suppression ou modification d'autres informations ;

- duplication, reproduction ou fac-similé ;
- efficacité des éléments de sécurité aux trois niveaux d'inspection : examen superficiel, examen au moyen d'un équipement simple par des inspecteurs qualifiés et inspection par des spécialistes judiciaires ;
- confiance et facilité d'authentification au deuxième niveau.

La protection contre ces menaces ou d'autres requiert le recours à un ensemble d'éléments et de techniques de sécurité, combinés de façon optimale dans le document. Certains éléments peuvent offrir une protection contre plusieurs types de menace, mais il n'en existe aucun qui puisse, à lui seul, protéger contre tous ces types de menaces. De même, aucun élément de sécurité n'est efficace à 100 % pour éliminer une catégorie quelconque de menace. La meilleure protection consiste à utiliser un ensemble équilibré d'éléments et de techniques formant plusieurs couches de sécurité intégrées dans le document, qui se combinent pour prévenir ou faire échouer toute attaque frauduleuse.

A.5 ÉLÉMENTS ET TECHNIQUES DE SÉCURITÉ

Dans les sections qui suivent, les éléments, techniques et autres mesures de sécurité sont classés selon les phases des processus de production et de personnalisation et les composants du document de voyage ainsi créé :

1) matériaux des supports ;
2) conception et impression de sécurité ;
3) protection contre la copie, la contrefaçon et la falsification ;
4) techniques de personnalisation.

Il est recommandé aux États émetteurs d'incorporer tous les éléments/mesures de sécurité de base et de sélectionner un certain nombre d'éléments/mesures de sécurité dans la liste d'éléments supplémentaires après avoir effectué une évaluation complète des risques auxquels sont exposés leurs documents de voyage. Sauf indication contraire, les éléments de sécurité s'appliquent à toutes les parties d'un document de voyage, y compris la couverture et la reliure du livret, et à toutes les pages intérieures d'un passeport, y compris la page de données personnelles, les pages de garde et les pages de visas. Il faut veiller soigneusement à ce que les éléments de sécurité ne compromettent pas la lisibilité par machine du document de voyage.

A.5.1 Matériaux des supports

A.5.1.1 Papier utilisé pour les pages d'un document de voyage

Éléments de sécurité de base :

- papier sans fluorescence sous UV, ou support à réponse sous UV contrôlée, tel qu'il présente, lorsqu'il est exposé au rayonnement UV, une fluorescence dont la couleur se distingue de la luminescence bleu-blanc utilisée dans les matériaux généralement disponibles sur le marché contenant des azurants optiques ;
- filigrane comprenant deux ou plusieurs niveaux de gris dans la page de données personnelles et les pages de visas ;

- réactifs chimiques appropriés dans le papier, au moins pour la page de données personnelles (si cela est compatible avec la technique de personnalisation) ;
- papier ayant des caractéristiques appropriées d'absorption, de rugosité et de faible déchirure de surface.

Éléments de sécurité supplémentaires :

- filigrane en repérage précis avec l'impression ;
- filigrane sur la page de renseignements différent de celui qui est utilisé sur les pages de visa pour empêcher la substitution de pages ;
- filigrane multiton (aussi appelé filigrane fabriqué à la forme ronde) ;
- fibres fluorescentes invisibles ;
- fibres (fluorescentes) visibles ;
- fil de sécurité (incrusté ou fenêtré) contenant des éléments de sécurité supplémentaires tels que microimpression et fluorescence ;
- marqueur conçu pour être détecté par un équipement spécial ;
- élément de sécurité perforé au laser.

A.5.1.2 Vignettes en papier ou sur d'autres supports utilisées pour la page de données personnelles d'un document de voyage

Éléments de sécurité de base :

- papier sans fluorescence sous UV, ou support à réponse sous UV contrôlée, tel qu'il présente, lorsqu'il est exposé au rayonnement UV, une fluorescence dont la couleur se distingue de la luminescence bleu-blanc utilisée dans les matériaux généralement disponibles sur le marché contenant des azurants optiques ;
- réactifs chimiques appropriés dans le papier (option normalement non applicable à une vignette à support plastique) ;
- fibres fluorescentes invisibles ;
- fibres (fluorescentes) visibles ;
- système d'adhésifs et/ou autres caractéristiques empêchant d'enlever la vignette sans causer de dommages visibles à la vignette et à tous les films ou revêtements de protection utilisés avec elle.

Éléments de sécurité supplémentaires :

- fil de sécurité (incrusté ou fenêtré) contenant des éléments de sécurité supplémentaires tels que microimpression et fluorescence ;
- le papier d'une page de renseignements produite sous forme de vignette peut être filigrané ;

- élément de sécurité perforé au laser ;
- motif de sécurité à l'intérieur de la vignette, découpé à l'emporte-pièce afin de mettre en évidence toute tentative d'altération.

A.5.1.3 Sécurité du papier utilisé pour la face intérieure de la couverture d'un passeport en livret

Il n'est pas nécessaire que le papier utilisé pour former la face intérieure de la couverture d'un passeport en livret soit filigrané. Si une face intérieure de la couverture est utilisée comme page de données personnelles (voir § A.5.5.1), ce qui n'est pas du tout recommandé, d'autres mesures doivent être utilisées pour fournir un niveau de sécurité contre tous les types d'attaques équivalant à celui qui serait assuré si la page de données personnelles était une page intérieure.

Lorsqu'une face intérieure de la couverture est utilisée comme page de données personnelles, le papier formant la face intérieure devrait contenir des réactifs chimiques appropriés. Le papier ainsi chimiquement sensibilisé devrait être compatible avec la technique de personnalisation et l'adhésif utilisé pour coller le papier de garde au matériau de la page de couverture du passeport.

A.5.1.4 Supports synthétiques

Lorsque le support utilisé pour la page de données personnelles d'un passeport en livret ou d'une carte DVLM est entièrement constitué de plastique ou d'une variante du plastique, il est généralement impossible d'y incorporer les éléments de sécurité indiqués dans les § A.5.1.1 à A.5.1.3. Dans ces cas, il faut inclure des propriétés de sécurité supplémentaires, notamment des éléments de sécurité imprimés additionnels, des techniques de personnalisation renforcées et l'emploi d'éléments optiquement variables en plus de ce qui est recommandé dans les § A.5.2 à A.5.5.2. Les États devraient de préférence s'assurer que le support plastique est fabriqué dans des conditions contrôlées et qu'il contient des propriétés distinctives (par exemple, fluorescence contrôlée) pour le distinguer des supports normalement employés pour les cartes de transactions financières.

Éléments de sécurité de base :

- la construction de la page de renseignements devrait empêcher la séparation physique en couches ;
- support sans fluorescence sous UV ou avec réponse sous UV contrôlée, tel qu'il présente, lorsqu'il est exposé au rayonnement UV, une fluorescence dont la couleur se distingue de la luminescence bleu-blanc utilisée dans les matériaux généralement disponibles sur le marché contenant des azurants optiques ;
- des mesures appropriées devraient être employées pour incorporer la page de renseignements de manière sûre et durable dans le DVLM ;
- élément optiquement variable.

Éléments de sécurité supplémentaires :

- élément fenêtré ou transparent ;
- élément tactile ;
- élément perforé au laser.

A.5.2 Impression de sécurité

A.5.2.1 Impression des fonds et des textes

Éléments de sécurité de base (voir 4.2 – Termes et définitions dans le Doc 9303-1) :

- motif du dessin de sécurité du fond en guillochis travaillé en deux tons[1] ;
- impression irisée ;
- texte en microimpression ;
- fond de sécurité des pages de données personnelles imprimé avec un dessin différent de celui des pages de visas ou des autres pages du document.

Éléments de sécurité supplémentaires :

- impression en taille douce unicolore ou multicolore comprenant un dessin en « lignes noires/lignes blanches » sur une ou plusieurs des feuilles de garde ou des pages de visas ;
- image latente (taille douce) ;
- motif anti-scan ;
- motif de sécurité en bichromie ;
- élément en relief (tridimensionnel) ;
- élément en repérage précis recto-verso (par transparence) ;
- erreur délibérée (par exemple, faute d'orthographe) incorporée au texte en microimpression ;
- chaque page de visa imprimée avec un dessin du fond de sécurité différent ;
- élément tactile ;
- fonte(s) unique(s).

A.5.2.2 Encres

Éléments de sécurité de base :

- encre fluorescente sous rayonnement UV (visible ou invisible) sur la page de données personnelles et sur toutes les pages de visas ;

1. Lorsque les guillochis sont générés par ordinateur, l'image reproduite sur le document doit être telle qu'aucune indication de structure en pixels ne soit discernable. Leur apparence peut être celle d'images positives, où les traits formant les images apparaissent comme étant imprimés avec des espaces blancs entre eux, ou d'images négatives, où ces traits apparaissent en blanc, avec entre eux des espaces imprimés. Dans les guillochis travaillés en deux tons, le motif est formé par superposition de deux éléments, reproduits en couleurs contrastantes.

- encres réactives, si les pages du document ou la vignette sont sur support papier, au moins pour la page de données personnelles (si c'est compatible avec la technique de personnalisation).

Éléments de sécurité supplémentaires :

- encres à propriétés optiquement variables ;
- encres métalliques ;
- encres de numérotation pénétrantes ;
- encres métamères ;
- encres invisibles dans l'infrarouge ;
- encres à absorption infrarouge ;
- encres phosphorescentes ;
- encres marquées ;
- encres invisibles fluorescentes en différentes couleurs lorsqu'elles sont exposées à différentes longueurs d'onde.

A.5.2.3 Numérotation

Il est fortement recommandé d'utiliser le numéro de document unique comme numéro de passeport.

Éléments de sécurité de base :

- le numéro de passeport doit figurer sur toutes les feuilles du document et sur la page de données personnelles du document ;
- le numéro du document doit être imprimé et/ou perforé ;
- le numéro de document figurant sur une vignette doit être imprimé dans un style particulier de chiffres ou de caractères et avec une encre d'impression fluorescente sous UV en plus d'avoir une couleur visible ;
- le numéro qui figure sur la page de renseignements d'un passeport fait d'un support synthétique ou sur une carte DVLM peut être incorporé par la même technique que celle qui est utilisée pour appliquer les données personnelles durant le processus de personnalisation ;
- dans le cas des cartes DVLM, le numéro devrait figurer sur les deux côtés.

Éléments de sécurité supplémentaires :

- lorsque le numéro est perforé, il est préférable d'utiliser une perforation laser. La perforation du numéro sur la page de renseignements est facultative mais, si elle est utilisée, il faut prendre soin de ne pas compromettre la clarté du portrait ou de la ZIV ni d'obstruer la ZLA de quelque façon que ce soit. Il est souhaitable de perforer la couverture du passeport ;

- lorsque le numéro est imprimé, il devrait l'être idéalement dans un style particulier de chiffres ou de caractères et avec une encre d'impression fluorescente sous UV en plus d'avoir une couleur visible.

A.5.2.4 Mesures de sécurité spéciales pour les pages de données personnelles non protégées

La surface de la page de renseignements doit être protégée contre la souillure durant son utilisation normale, y compris la lecture automatique régulière de la ZLA, et contre la falsification.

Si une page d'un document est utilisée pour des données personnelles non protégées par une couche protectrice (un film ou un revêtement de sécurité) (voir les § A.5.3.2, A.5.4.3 et A.5.4.4), une protection supplémentaire doit être assurée par l'emploi de l'impression taille douce, en y incorporant une image latente et du texte en microimpression, et en utilisant de préférence une encre de couleur changeante (par exemple, encre à propriétés optiquement variables).

A.5.2.5 Mesures de sécurité spéciales pour les cartes et les pages de données personnelles en plastique

Lorsqu'un document de voyage est entièrement fait de plastique, il faut employer des éléments de sécurité optiquement variables, c'est-à-dire des éléments dont l'apparence change selon l'angle d'observation. Ces éléments peuvent être des images latentes, des éléments lenticulaires, une encre de couleur changeante ou des images diffractives optiquement variables (DOVID).

A.5.3 Protection contre la copie

A.5.3.1 Nécessité d'une protection anticopie

L'état de développement actuel des techniques de reproduction numérique généralement disponibles et le risque de fraude qui en résulte signifient qu'il faut utiliser des éléments de sécurité de haute qualité, sous forme d'éléments optiquement variables ou d'autres dispositifs équivalents, comme protection contre la copie et le scannage. Il convient de souligner l'importance de sécuriser la page de données personnelles d'un passeport en livret, d'une carte de voyage ou d'un visa, en utilisant une technologie indépendante et complexe d'éléments optiquement variables ou d'autres dispositifs équivalents, en complément d'autres techniques de sécurité. Il faudrait notamment mettre l'accent sur les éléments facilement identifiables, visuels ou tactiles examinés lors d'une inspection de niveau 1.

L'intégration judicieuse de composants optiquement variables ou d'autres dispositifs équivalents dans la structure en couches de la page de données personnelles devrait aussi protéger les données contre l'altération frauduleuse. Il faut également protéger contre la contrefaçon les composants optiquement variables et tous les matériaux de sécurité connexes utilisés pour créer la structure en couches.

A.5.3.2 Méthodes de protection anticopie

Sous réserve des recommandations minimales indiquées dans les § A.5.4.3 et A.5.4.4 concernant la nécessité de recourir au laminage, il convient d'employer des dispositifs optiquement variables comme *éléments de sécurité de base* sur la page de données personnelles d'un passeport en livret, d'une carte de voyage ou d'un visa.

Lorsqu'une page de données personnelles d'un passeport en livret, d'une carte de voyage ou d'un visa est protégée par un film ou un revêtement de sécurité, il convient d'y incorporer un élément optiquement variable (basé de préférence sur une structure diffractive mettant en évidence toute tentative d'altération). L'élément employé ne doit pas compromettre la lisibilité des données introduites.

Lorsque la page de données personnelles est une vignette papier encapsulée ou une page d'un passeport, les données personnelles doivent être convenablement protégées par un film de sécurité ou d'autres mesures assurant une sécurité équivalente afin d'empêcher qu'elles ne soient altérées ou supprimées.

Lorsque la page de données personnelles lisible par machine d'un passeport en livret est entièrement constituée d'un support synthétique, il convient d'y incorporer un élément optiquement variable. Pour accroître le niveau de protection contre la reproduction, il est recommandé d'inclure un élément diffractif optiquement variable.

Au lieu d'un élément optiquement variable, il est possible d'utiliser des éléments fenêtrés ou transparents, des éléments perforés au laser ou d'autres éléments considérés comme offrant une protection équivalente.

Si le document de voyage n'est pas protégé par un revêtement ou un film de sécurité, il faut utiliser un élément optiquement variable (basé de préférence sur une structure diffractive) avec une surimpression en taille douce ou une autre technique d'impression.

A.5.4 Techniques de personnalisation

A.5.4.1 Personnalisation des documents

Il s'agit du processus par lequel le portrait, la signature et/ou d'autres données personnelles du titulaire du document sont appliqués au document de voyage. Ces données, qui enregistrent les renseignements personnalisés concernant le titulaire, sont les plus exposées au risque de contrefaçon ou d'altération frauduleuse. Un des types de fraude les plus fréquents consiste à enlever le portrait figurant sur un document de voyage volé ou obtenu illégalement et à le remplacer par le portrait d'une autre personne. Les documents portant une photographie collée sont particulièrement vulnérables à la substitution de photographie. L'emploi de photographies collées N'est donc PAS autorisé dans les DVLM.

A.5.4.2 Protection contre l'altération

Pour assurer une bonne sécurisation contre les tentatives de falsification ou d'altération frauduleuse, il est fortement recommandé d'intégrer dans le matériau de base du document les données personnelles, y compris le portrait, la signature (si elle figure sur la page de données personnelles) et les principaux renseignements sur la délivrance. Il existe diverses technologies permettant de personnaliser ainsi le document, notamment celles qui sont indiquées ci-après. Cette liste n'exclut pas le développement de nouvelles technologies et ne correspond pas à un ordre d'importance particulier :

- impression laser ;
- impression par transfert thermique ;
- impression au jet d'encre ;
- procédés photographiques ;
- gravure laser.

Les mêmes technologies peuvent aussi être employées pour appliquer des données sur la page d'observations du passeport. L'impression laser ne doit pas être utilisée pour personnaliser des visas ou d'autres documents de sécurité qui ne sont pas protégés par un film de sécurité.

Les autorités devraient tester leurs processus et techniques de personnalisation contre les méfaits.

A.5.4.3 Choix du système de documents

Le choix d'une technologie particulière est une question qui relève de chaque État émetteur ; il dépend d'un certain nombre de facteurs tels que le volume de documents de voyage à produire, la construction du document et la réalisation de la personnalisation pendant ou après le processus d'assemblage du document ou du livret passeport et selon que la délivrance des passeports est centralisée ou décentralisée.

Quelle que soit la méthode choisie, il est essentiel de prendre des précautions pour protéger les détails de la personnalisation contre les tentatives d'altération. Ces précautions sont importantes même si l'élimination des portraits collés réduit le risque de substitution de photographie, car les données personnelles non protégées restent vulnérables à l'altération. Il est nécessaire de protéger ces données au moyen d'un film de sécurité thermocollé (ou l'équivalent) doté de propriétés frangibles ou par l'application d'une technologie équivalente qui met en évidence toute tentative d'altération.

A.5.4.4 Protection contre la substitution de photographie et l'altération de données sur la page de données personnelles d'un passeport en livret

Éléments de sécurité de base :

- personnalisation du portrait et de toutes les données personnelles par leur intégration dans le matériau de base ;
- le fond imprimé de sécurité (par exemple, guillochis) doit couvrir la zone du portrait ;
- utilisation d'encres réactives et de réactifs chimiques dans le papier ;
- un dispositif de sécurité visible devrait déborder sur le portrait sans en obstruer la visibilité ; il est recommandé d'utiliser un élément optiquement variable ;
- utilisation d'un film de sécurité thermoscellé (ou l'équivalent) ou la combinaison d'une technologie de personnalisation et de matériau de support assurant une résistance équivalente à la substitution et/ou à la contrefaçon du portrait et d'autres données personnelles.

Éléments de sécurité supplémentaires :

- la signature affichée du titulaire peut être scannée et incorporée dans l'impression ;
- image stéganographique incorporée dans le document ;
- portrait(s) supplémentaire(s) du titulaire ;
- éléments vérifiables par machine conformes au Doc 9303, Parties 9 à 12.

A.5.5 Mesures de sécurité supplémentaires pour passeports en livret

A.5.5.1 Position de la page de données personnelles

Il est recommandé que les États placent les données personnelles sur une page intérieure (la deuxième ou l'avant-dernière page). Lorsque la page de données personnelles est placée sur la face intérieure de la couverture du PLM, elle risque de faire l'objet d'attaques frauduleuses, le plus souvent par substitution de la photo ou de la page complète, en

raison de la méthode habituelle de fabrication des couvertures de passeport. Un État émetteur peut néanmoins mettre la page de données personnelles sur une page de couverture à condition de veiller à ce que la construction de la couverture offre un niveau de protection contre la fraude similaire à celui qui est associé aux pages intérieures. Il est néanmoins fortement DÉCONSEILLÉ de placer la page de données personnelles sur la couverture.

A.5.5.2 Substitution de page complète

L'attention des États émetteurs est appelée sur le fait que, depuis le remplacement des photographies collées dans les passeports par des pages de données personnelles intégrées, il a été constaté des cas de substitution de page complète dans lesquels la page de données personnelles du passeport était enlevée et remplacée entièrement par une page frauduleuse. Bien que la substitution d'une page entière soit généralement plus difficile à réaliser que celle d'une photographie collée, il importe d'adopter les recommandations suivantes pour se prémunir contre cette catégorie de risque. Comme pour toutes les autres catégories de falsification de documents, il est préférable d'employer une combinaison d'éléments de sécurité pour assurer la protection contre la substitution de page complète plutôt que de se fier à un seul élément qui, s'il était défaillant, pourrait compromettre la sécurité de l'ensemble du document de voyage.

Éléments de sécurité de base :

- la technique de couture qui relie les pages en livret doit être telle qu'il soit difficile de retirer une page sans laisser une trace évidente de ce qui est arrivé ;
- fond de sécurité de la page de données personnelles imprimé avec un dessin différent de celui qui est employé pour les pages de visas ;
- numéros de page intégrés dans le dessin de sécurité des pages de visas ;
- numéro de série sur chaque feuille, de préférence perforé.

Éléments de sécurité supplémentaires :

- fil à coudre multicolore et/ou, notamment, fluorescent sous UV ;
- motif programmable de couture au fil ;
- colle durcie sous UV appliquée à la couture ;
- repères ou marques de collationnement imprimés sur la tranche de chaque page de visa ;
- éléments de sécurité perforés au laser sur la page de données personnelles ;
- données personnelles imprimées sur une page intérieure en plus de la page de renseignements.

Si des vignettes autocollantes sont utilisées, il est conseillé d'appliquer les éléments de sécurité supplémentaires indiqués dans les § A.5.1.2 et A.5.2.4, notamment l'emploi du numéro de document de voyage pour établir un lien entre la vignette et le DVLM.

A.5.6 Contrôle de la qualité

Des vérifications et contrôles de la qualité à tous les stades du processus de production, ainsi que d'un lot au suivant, sont indispensables pour assurer l'uniformité des documents de voyage finis. Ils devraient inclure des vérifications d'assurance de la qualité de tous les matériaux utilisés dans la fabrication des documents et de la lisibilité des lignes de

lecture automatique. Il est capital que les documents de voyage finis soient tous semblables, car les inspecteurs de l'immigration et les agents du contrôle aux frontières se fient à la possibilité de reconnaître les faux documents par des variations de leur apparence ou de leurs caractéristiques. L'existence de variations dans la qualité, l'apparence ou les caractéristiques des documents de voyage authentiques d'un État compliquerait la détection des documents contrefaits ou falsifiés.

A.5.7 Contrôle de la sécurité de la production et des produits

Une menace grave contre la sécurité des PLM d'un État émetteur peut résulter de l'enlèvement non autorisé, des locaux de production, de PLM authentiques finis mais non personnalisés ou de composants permettant de fabriquer des PLM.

A.5.7.1 Protection contre le vol et l'usage abusif de documents ou de composants de documents vierges authentiques

Les documents vierges devraient être entreposés dans des locaux verrouillés et bien surveillés. Il convient d'adopter les mesures de sécurité suivantes :

Mesures de sécurité de base :

- bonne sécurité physique des locaux avec contrôle de l'accès aux zones de livraison, d'expédition et de production et aux installations d'entreposage des documents ;
- piste de vérification complète, avec comptage et rapprochement de tous les matériaux (utilisés, non utilisés, défectueux ou gâchés) et relevés certifiés de ces matériaux ;
- numérotation par série de tous les documents vierges et des composants critiques du point de vue de la sécurité avec piste de vérification complète pour chaque document de la fabrication jusqu'à l'expédition, selon le cas ;
- s'il y a lieu, suivi et numéros de contrôle des autres composants principaux des documents (par exemple, rouleaux ou feuilles de laminage, éléments optiquement variables) ;
- véhicules sécurisés pour le transport des documents vierges et des principaux composants des documents (s'il y a lieu) ;
- communication rapide, entre les gouvernements et avec les autorités de contrôle frontalier, d'informations détaillées sur tous les documents de voyage vierges perdus ou volés et consignation de
  ces informations dans la base de données d'INTERPOL sur les documents perdus ou volés ;
- mise en place de contrôles appropriés pour protéger les procédures de production contre toute fraude interne ;
- contrôle de sécurité du personnel.

Mesures de sécurité supplémentaires :

- surveillance/enregistrement de toutes les zones de production par télévision en circuit fermé, lorsque c'est autorisé ;

- centralisation de l'entreposage et de la personnalisation des documents dans le plus petit nombre d'endroits possible.

Tableau A-1. Tableau récapitulatif des recommandations relatives à la sécurisation

Éléments	*Éléments de sécurité de base*	*Éléments de sécurité supplémentaires*
Matériaux des supports (A.5.1)		
Supports papier (A.5.1.1)	– réponse sous UV contrôlée – filigrane à deux tons – réactifs chimiques – caractéristiques d'absorption et de surface appropriées	– filigrane en repérage précis – filigrane différent sur la page de données personnelles et la page de visa – filigrane multiton – fibres fluorescentes invisibles – fibres (fluorescentes) visibles – fil de sécurité – marqueur – élément de sécurité perforé au laser
Vignette en papier ou sur d'autres supports (A.5.1.2)	– réponse sous UV contrôlée – réactifs chimiques – fibres fluorescentes invisibles – fibres (fluorescentes) visibles – système d'adhésifs	– fil de sécurité – filigrane – élément de sécurité découpé à l'emporte-pièce
Supports synthétiques (A.5.1.4)	– construction empêchant la séparation en couches – support sans fluorescence – incorporation sécurisée de la page de renseignements – éléments optiquement variables – voir § A.5.2 – A.5.5, selon le cas	– élément fenêtré ou transparent – élément tactile – élément perforé au laser
Impression de sécurité (A.5.2)		
Impression des fonds et des textes (A.5.2.1)	– fond guillochis bicolore – impression irisée – texte en microimpression – conception unique de la page de renseignements	– impression en taille douce – image latente – motif anti-scan – motif de sécurité en bichromie – élément en relief – élément en repérage précis recto-verso – erreur délibérée – dessin unique sur chaque page – élément tactile – fonte(s) unique(s)

Éléments	*Éléments de sécurité de base*	*Éléments de sécurité supplémentaires*
Encres (A.5.2.2)	– encre fluorescente sous UV – encres réactives	– encres à propriétés optiquement variables – encres métalliques – encres de numérotation pénétrantes – encres métamères – encres invisibles dans l'infrarouge – encres à absorption infrarouge – encres phosphorescentes – encres marquées – encres invisibles
Numérotation (A.5.2.3)	– numérotation de toutes les feuilles – numéro imprimé ou perforé – caractères spéciaux pour les numéros des vignettes – même technique utilisée pour l'application des numéros et des données personnelles sur les supports synthétiques et les cartes	– numéro de document perforé au laser – caractères spéciaux
Techniques de personnalisation (A.5.4)		
Protection contre la substitution de photographie et l'altération (A.5.4.4)	– données personnelles intégrées – fond de sécurité débordant sur la zone du portrait – encres réactives et réactifs chimiques dans le papier – dispositif de sécurité visible débordant sur la zone du portrait – film de sécurité thermoscellé ou l'équivalent	– signature affichée – image stéganographique – portrait(s) supplémentaire(s) – élément biométrique conforme à la Partie 9
Mesures de sécurité supplémentaires pour passeports en livret (A.5.5)		
Substitution de page (A.5.5.2)	– technique de couture sécurisée – fil à coudre fluorescent sous UV – dessin unique sur la page de renseignements – numéros de page intégrés dans le dessin de sécurité – numéro de série sur chaque feuille	– fil à coudre multicolore – motif de couture programmable – colle durcie sous UV appliquée à la couture – repères de collationnement sur chaque page – élément de sécurité perforé au laser – données personnelles sur une page intérieure

Éléments	*Éléments de sécurité de base*	*Éléments de sécurité supplémentaires*
Contrôle de la sécurité de la production et des produits (A.5.7)		
Protection contre le vol et l'usage abusif (A.5.7.1)	– bonne sécurité physique – piste de vérification complète – numéros de série de tous les documents vierges, s'il y a lieu – suivi et numéros de contrôle des composants, s'il y a lieu – transport sécurisé des documents vierges – échange international de renseignements sur les documents perdus ou volés – procédures de protection contre la fraude interne – contrôle de sécurité du personnel	– télévision en circuit fermé dans les zones de production – centralisation de l'entreposage et de la personnalisation

Note 1.— La liste des éléments supplémentaires n'est pas exhaustive ; les États émetteurs et les organisations émettrices sont encouragés à adopter d'autres éléments de sécurité qui ne sont pas mentionnés explicitement dans le présent appendice.

Note 2.— Les descriptions qui figurent dans le Tableau A-1 sont nécessairement abrégées par rapport au texte principal. Pour faciliter la consultation, les paragraphes correspondant aux sections du présent appendice sont indiqués par les numéros figurant entre parenthèses dans la colonne « Éléments » du tableau.

Note 3.— Certains éléments sont répétés une ou plusieurs fois dans le tableau, ce qui signifie qu'ils protègent contre plus d'un type de menace. Il n'est nécessaire de les introduire qu'une seule fois dans un document donné.

Note 4.— Il existe de nombreux autres facteurs applicables à la sécurité des passeports qui ne sont pas décrits ici. Les Appendices B et C donnent des orientations supplémentaires. Les Appendices A, B et C doivent donc être utilisés ensemble pour assurer l'intégrité de la délivrance des documents.

Note 5.— Toute mention, explicite ou implicite, de termes et/ou de technologies spécifiques ne se rapporte qu'à l'aspect générique des termes ou des technologies et ne vise aucun vendeur ni aucun fournisseur de technologie en particulier.

— — — — — — — —

APPENDICE B À LA PARTIE 2
(INFORMATIF)

VÉRIFICATION DE SÉCURITÉ DES DOCUMENTS ASSISTÉE PAR MACHINE

B.1 PORTÉE

Le présent appendice contient des recommandations sur l'authentification par machine des éléments de sécurité contenus dans le document lui-même (authentification basée sur les matériaux utilisés, l'impression de sécurité et les techniques de protection anticopie) ainsi que des orientations sur les technologies de lecture qui permettent l'authentification des documents par machine.

B.2 LECTEURS DE DOCUMENTS ET SYSTÈMES D'AUTHENTIFICATION PAR MACHINE

Pour vérifier les éléments de sécurité traditionnels et nouveaux des DVLM, il est important de mettre en place une technologie de lecture capable de prendre en charge la grande variété de documents de voyage en circulation. Ces lecteurs doivent être équipés de capteurs appropriés pour lire les éléments d'authentification par machine les plus courants et les plus évolués. Il s'agit évidemment d'une question de coûts et d'infrastructure à l'échelle mondiale.

B.2.1 Lecteurs standards

Les lecteurs standards déployés aux frontières sont habituellement munis des capteurs suivants :

- dispositif d'éclairage en mode visible (VIS), UV et IR et de saisie d'images haute résolution (résolution minimale de 300 dpi), ce qui permet de lire la ZLA (de préférence dans la région IR du spectre) et le traitement d'image d'autres éléments (dans la région VIS du spectre) ;
- lecteurs de CI sans contact conformes à la norme ISO 14443 (à une fréquence de 13,56 MHz).

En général, les lecteurs standards sont capables de détecter et de vérifier les éléments de sécurité suivants :

- lecture de la ZLA et vérification du chiffre de contrôle ;
- lecture du CI sans contact et authentification passive (et, à titre facultatif, authentification active) ;
- vérifications de sécurité génériques (papier sans fluorescence sous UV, ZLA lisible sous IR, etc.).

Les autres caractéristiques « intelligentes » de ces lecteurs dépendent uniquement du logiciel, non de capteurs supplémentaires, et peuvent donc être facilement déployées à la discrétion de l'État récepteur sans qu'il soit nécessaire d'engager d'autres dépenses pour acquérir un équipement spécialisé. Les capacités logicielles des lecteurs peuvent notamment comprendre les éléments suivants :

- reconnaissance des formes en utilisant des bases de données (basée sur des images VIS, UV et IR) ;
- lecture et authentification de filigranes numériques (éléments stéganographiques) pour vérifier l'authenticité de la délivrance ;
- détection et lecture d'affichages (alphanumériques) et leurs futurs éléments de sécurité ;
- détection et lecture d'éléments de sécurité basés sur la technologie du support plastique avec diode électroluminescente (DEL).

B.2.2 Lecteurs évolués

Les lecteurs évolués peuvent en outre être équipés des capteurs suivants, capables d'authentifier des éléments de sécurité spéciaux :

- lumière coaxiale pour la vérification de revêtements de sécurité rétroréfléchissants ;
- éclairage par diode laser ou DEL pour la vérification d'éléments de structure spéciaux, par exemple, les DOVID ;
- capteurs magnétiques pour des éléments de support spéciaux, par exemple, pour la vérification des fibres magnétiques ;
- dispositifs d'analyse spectrale ou de détection de polarisation ;
- éclairage par lumière transmise de la page de renseignements du PLM pour la vérification des filigranes en repérage précis, des perforations laser, des éléments fenêtrés et des motifs en repérage par transparence — requiert une géométrie de lecture spéciale pour permettre de placer la page de renseignements (sans couverture derrière) sur le lecteur.

Les fonctions de lecture évoluées sont habituellement fondées sur des accords nationaux, bilatéraux, multilatéraux ou propriétaires et exigent un matériel spécialisé.

B.2.3 Systèmes de référence, infrastructure à clés publiques (ICP)

Pour authentifier certains types d'éléments vérifiables par machine, il peut être nécessaire d'utiliser un système de référence ou une ICP. Il peut s'agir de l'ICP de DVLM existante [le répertoire de clés publiques (RCP) de l'OACI étant la partie la plus importante], où les États peuvent échanger des renseignements sur leurs éléments de sécurité dans le cadre de la structure de données logique (SDL), sécurisée au moyen de certificats.

B.3 ÉLÉMENTS DE SÉCURITÉ ET LEUR APPLICATION À L'AUTHENTIFICATION PAR MACHINE

Les tableaux qui suivent décrivent les principaux éléments et les principales techniques de sécurité indiqués à l'Appendice A (normes de sécurité) et expliquent comment l'authentification par machine pourrait être utilisée pour ces mécanismes de sécurité. Les autorités émettrices qui choisissent des éléments de sécurité indiqués à l'Appendice A peuvent employer ces tableaux pour vérifier les possibilités d'authentification par machine de ces éléments.

B.3.1 Matériaux des supports

B.3.1.1 Papier utilisé pour les pages d'un document de voyage

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Réponse sous UV contrôlée		X					Intensité UV
Filigrane à deux tons					Transmission	F	Appariement des formes
Réactifs chimiques							s.o.
Caractéristiques appropriées d'absorption et de surface							s.o.
Éléments supplémentaires							
Filigrane en repérage précis					Transmission	F	Appariement des formes
Filigrane différent sur la page de renseignements et la page de visa					Transmission	F	Appariement des formes*
Filigrane multiton					Transmission	F	Appariement des formes
Fibres fluorescentes invisibles		X	X			F/V	Appariement des formes
Fibres (fluorescentes) visibles	X	X				F/V	Appariement des formes
Fil de sécurité	X	X			Transmission, magnétique	F	Appariement des formes
Marqueur					Spécial	F/V	Dépend du marqueur
Élément de sécurité perforé au laser					Transmission	F/V	Appariement des formes

* Requiert l'interaction de l'utilisateur et n'est pas adapté aux systèmes de contrôle frontalier automatisé.

B.3.1.2 Vignettes en papier ou sur d'autres supports

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Réponse sous UV contrôlée		X					Intensité UV
Réactifs chimiques							s.o.
Fibres fluorescentes invisibles		X	X			F/V	Appariement des formes
Fibres (fluorescentes) visibles	X	X				F/V	Appariement des formes
Système d'adhésifs							s.o.
Éléments supplémentaires							
Fil de sécurité	X				Transmission, magnétique	F	Appariement des formes
Filigrane					Transmission	F	s.o.
Élément de sécurité perforé au laser					Transmission	F/V	Appariement des formes
Motif de sécurité découpé à l'emporte-pièce					Transmission	F	Appariement des formes

B.3.1.3 Supports synthétiques

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Construction empêchant la séparation en couches							s.o.
Matériau sans fluorescence		X					Intensité UV
Incorporation sécurisée de la page de renseignements							s.o.

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments optiquement variables							Voir § A.5.3
Voir § A.5.2 – A.5.5, selon le cas							
Éléments supplémentaires							
Élément fenêtré ou transparent					Transmission	F	Appariement des formes
Élément tactile					Rétroréfléchissant	F/V	Appariement des formes
Élément perforé au laser					Transmission	F/V	Appariement des formes
Caractéristiques de surface	X		X		Rétroréfléchissant	F	Appariement des formes

B.3.2 Impression de sécurité

B.3.2.1 Impression des fonds et des textes

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Fond en guillochis bicolore	X	X	X			F	Appariement des formes
Impression irisée	X	X			Caméra haute résolution	F	Appariement des formes
Texte en microimpression	X	X	X		Caméra haute résolution	F	Appariement des formes
Dessin unique sur la page de renseignements	X					F	Appariement des formes
Éléments supplémentaires							
Impression en taille douce	X	X	X			F	Appariement des formes*
Image latente							s.o.

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Motif anti-scan	X				Caméra haute résolution	F	Appariement des formes
Motif de sécurité en bichromie					Transmission	F	Appariement des formes*
Élément en relief					Rétroréfléchissant	F	Appariement des formes
Élément en repérage précis recto-verso					Transmission	F	Appariement des formes
Erreur délibérée	X	X	X			F	ROC, Appariement des formes
Dessin unique sur chaque page	X	X				F	Appariement des formes**
Élément tactile					Rétroréfléchissant	F	Appariement des formes
Fonte(s) unique(s)	X	X	X				Appariement des formes

* Mise en œuvre peu pratique pour les lecteurs de passeports.
** Requiert l'interaction de l'utilisateur et n'est pas adapté aux systèmes de contrôle frontalier automatisé.

B.3.2.2 Encres

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Encre fluorescente sous UV		X				F/V	Appariement des formes
Encres réactives					Spécial		Selon l'encre
Éléments supplémentaires							
Encres à propriétés optiquement variables	X				Éclairage variable	F/V	Appariement des formes

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Encres métalliques			X			F/V	Appariement des formes
Encres de numérotation pénétrantes					Spécial	V	Appariement des formes sur les deux côtés
Encres métamères	X	X	X			F	Filtres optiques et appariement des formes
Encres invisibles dans l'infrarouge	X		X			F/V	Appariement des formes
Encres à absorption infrarouge			X			F/V	Appariement des formes
Encres phosphorescentes		X	X			F/V	Appariement des formes
Encres marquées					Spécial	F	Appariement des formes
Encres invisibles		X	X			F	Appariement des formes
Encres magnétiques					Magnétique	F/V	Appariement des formes
Encres anti-stokes			X			F/V	Filtres optiques et appariement des formes

B.3.2.3 Numérotation

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Numérotation de toutes les feuilles Numéro imprimé et/ou perforé	X		X			F/V	ROC, Appariement des formes

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Caractères spéciaux pour les numéros des vignettes	X		X			F/V	ROC, Appariement des formes
Même technique utilisée pour l'application des numéros et des données personnelles sur les supports synthétiques et les cartes							s.o.
Éléments supplémentaires							
Numéro de document perforé au laser					Transmission	F/V	Appariement des formes
Fontes spéciales	X					F/V	ROC, Appariement des formes

B.3.3 Protection contre la copie

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Éléments optiquement variables sur la page de données personnelles	X				Éclairage variable	F/V	Appariement des formes
Dispositif optiquement variable (DOV) avec surimpression en taille douce s'il n'y a pas de film de sécurité							s.o.
Éléments supplémentaires							
Élément diffractif optiquement variable lisible par machine					Laser	F/V	Décodage
Élément de sécurité perforé au laser					Transmission	F/V	Appariement des formes
Motif anti-scan	X				Caméra haute résolution	F	Appariement des formes

B.3.4 Techniques de personnalisation

B.3.4.1 Protection contre la substitution de photographie et l'altération

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Données personnelles intégrées							s.o.
Fond de sécurité débordant sur la zone du portrait							s.o.
Encres réactives et réactifs chimiques dans le papier							s.o.
Dispositif de sécurité visible débordant sur la zone du portrait	X				Éclairage variable	F/V	Appariement des formes
Film de sécurité thermoscellé ou l'équivalent	X					F/V	Appariement des formes
Éléments supplémentaires							
Signature affichée							s.o.
Élément stéganographique	X	X	X			F/V	Décodage
Portrait(s) supplémentaire(s)	X	X	X	X		V	Appariement des formes
Élément biométrique conforme à la Partie 9				X		V	Lecteur RF

B.3.5 Mesures de sécurité supplémentaires pour passeports en livret

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Technique de couture sécurisée							s.o.
Fil à coudre fluorescent sous UV		X				F	Appariement des formes

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Dessin unique sur la page de renseignements	X					F	Appariement des formes
Numéros de page intégrés dans le dessin de sécurité	X	X			Caméra haute résolution		Appariement des formes
Numéro de série sur chaque feuille							s.o.
Éléments supplémentaires							
Fil à coudre multicolore	X	X				F	Appariement des formes
Motif de couture programmable	X	X				F	Appariement des formes
Colle durcie sous UV appliquée à la couture							s.o.
Repères sur chaque page							s.o.
Élément de sécurité perforé au laser					Transmission	F/V	Appariement des formes
Données personnelles sur une page intérieure							s.o.

B.3.6 Mesures de sécurité supplémentaires adaptées à l'authentification par machine

Les éléments de sécurité suivants conviennent à l'authentification par machine mais ne figurent pas dans la liste de l'Appendice A.

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Éléments de base							
Lecture de la ZLA et vérification du chiffre de contrôle	X		X			F/V	Calcul du total de contrôle
Lecture de CI sans contact et authentification passive (+AA)				X			Lecteur RF

Éléments de sécurité	*Capteur requis pour l'authentification par machine*					*Motif fixe/variable*	*Méthode d'authentification par machine*
	Lecteur standard				*Lecteur évolué*		
	VIS	*UV*	*IR*	*RF*	*Capteur spécial*		
Détection et lecture d'éléments de sécurité basés sur le support plastique avec DEL	X	X	X	X		F/V	DEL activée par R/F
Détection et lecture d'affichages (alphanumériques) et leurs futurs éléments de sécurité	X	X	X	X		F/V	Affichages activés par R/F
Détection et vérification d'éléments rétroréfléchissants	X				Lumière coaxiale	F/V	Appariement des formes
Codes à barres	X	X	X			V	Décodage

B.4 CRITÈRES DE SÉLECTION DES ÉLÉMENTS DE SÉCURITÉ VÉRIFIABLES PAR MACHINE

Les États émetteurs qui envisagent d'incorporer dans leurs DVLM des éléments de sécurité destinés à être authentifiés par machine et les États récepteurs qui prévoient de déployer des systèmes de lecture capables d'authentifier les DVLM par machine doivent tenir compte de plusieurs critères pour choisir ces éléments.

Ces critères sont analogues à ceux du processus de sélection des éléments biométriques à interopérabilité mondiale ou de la technologie de stockage des données, et comprennent les points suivants :

- sécurité — le critère le plus important ;
- disponibilité, mais exclusivité pour les documents de sécurité (il doit de préférence y avoir plus d'un fournisseur) ;
- double utilisation, c'est-à-dire l'élément sert à autre chose qu'à l'authentification par machine, par exemple, propriété générale anticopie ou inspection visuelle ;
- possibilité de personnaliser (c'est-à-dire d'individualiser) l'élément d'authentification par machine avec des renseignements du passeport pour sécuriser les données personnelles (par exemple, le numéro de passeport, le nom) afin d'éviter la réutilisation de parties de passeports authentiques ;
- compatibilité avec les processus de délivrance des DVLM ;
- compatibilité (avec les propriétés existantes et normalisées des DVLM) ;
- compatibilité avec les processus de contrôle aux frontières et ailleurs (par exemple, pas d'obstruction des éléments de sécurité de base, pas de temps supplémentaire nécessaire) ;
- interopérabilité ;
- disponibilité des capteurs ;

- coût (pour l'élément et le capteur) ;
- questions de propriété intellectuelle (par exemple, brevets) ;
- inspection primaire par rapport à inspection secondaire ;
- temps requis pour vraiment utiliser l'élément ;
- difficultés éventuelles que peuvent présenter les processus de fabrication et/ou de personnalisation du livret ;
- durabilité, c'est-à-dire selon les spécifications de l'ISO et de l'OACI applicables aux DVLM.

— — — — — — — —

APPENDICE C À LA PARTIE 2
(INFORMATIF)

AUTHENTIFICATION PAR LECTEUR OPTIQUE

C.1 INTRODUCTION

Pour l'authentification des documents de voyage lisibles à la machine (DVLM) dans le cadre du contrôle fixe aux frontières, y compris les portes ABC, l'utilisation des systèmes informatiques, qui vont au-delà de la simple extraction et de la vérification de la zone de lecture automatique (ZLA) des documents et de l'inspection automatique des éléments optiques de sécurité, augmente. Les améliorations majeures apportées aux technologies utilisées dans le cadre de l'authentification des documents par les machines a contribué à l'augmentation du nombre et de la diversité des systèmes d'authentification. Cependant, l'augmentation significative du nombre de voyageurs reste un défi pour tous les acteurs impliqués dans la conception, la production et le déploiement des systèmes d'authentification et des DVLM.

Les systèmes d'authentification utilisés pour effectuer l'authentification par machine des DVLM comprennent plusieurs composants qui doivent interagir correctement les uns avec les autres. En outre, les éléments de sécurité des documents lisibles par machine doivent être conçus et mis en œuvre en fonction des capacités des systèmes d'authentification et des connaissances des praticiens expérimentés.

Le présent Appendice fournit une série de recommandations pour les principales parties participant à la conception, à la mise en œuvre et à l'exploitation des systèmes et des éléments clés concernés, les principaux objectifs étant les suivants :

- accroître la sensibilisation aux questions de sécurité liées à l'authentification par machine, en associant les principales parties prenantes, par exemple les producteurs de documents de sécurité, les fabricants d'équipements de lecture et les pouvoirs publics ;
- proposer un catalogue de routines de contrôle génériques avec une terminologie cohérente ;
- définissent des recommandations pour les concepteurs de documents de sécurité, les fabricants de systèmes d'authentification et les niveaux opérationnels.

Le présent Appendice vise à aider les spécialistes à concevoir et à développer des systèmes d'authentification. Il est toutefois important de garder à l'esprit que le système d'authentification doit être utilisé pour faciliter l'arbitrage de son opérateur[1], et ne doit pas être considéré comme le seul décideur, notamment en ce qui concerne les éléments de sécurité qui ne peuvent pas être vérifiés par la machine et ne peuvent l'être que par un opérateur.

Le présent Appendice ne traite que de la partie optique de l'authentification des DVLM, et le champ d'application des recommandations est limité aux données acquises par des lecteurs de pages complètes, c'est-à-dire des images en taille réelle du document, comme décrit dans l'Appendice B de la présente partie. En outre, les lignes directrices ne font pas de distinction entre les inspections de 1er, 2e et 3e niveau, car les lecteurs de pages complètes peuvent être utilisés dans chacun de ces scénarios. Dans l'ensemble, les dispositifs mobiles ne sont (jusqu'à présent) pas pris en compte en

1. Opérateur : Une personne qui interagit directement avec le système d'authentification (par exemple, une interaction manuelle avec le lecteur de documents) dans le cadre d'un contrôle de documents.

raison de leurs capacités optiques limitées par rapport aux différentes sources de lumière (ni UV ni IR) et ne répondent donc pas aux exigences proposées.

Les bases et la terminologie nécessaires à une meilleure compréhension de l'authentification par lecteur optique sont présentées dans le § C.2. La question de l'harmonisation et de la normalisation des routines de contrôle est abordée dans le § C.3, où un catalogue de procédures de contrôle génériques est défini. Dans le § C.4, l'accent est mis sur les recommandations élaborées à l'intention des fabricants de systèmes d'authentification, et le § C.5 met en évidence plusieurs approches et méthodologies liées au traitement des données conformément aux politiques de protection des données.

C.1.1 Terminologie

Bien que les recommandations et les lignes directrices ne soient pas contraignantes pour les parties directement concernées, la terminologie a été adoptée et intégrée dans la partie 1 du Doc 9303 afin de fournir une description sans ambiguïté de ce qui doit être observé pour atteindre les objectifs définis dans le présent document.

La terminologie doit être considérée comme un moyen pratique d'organiser les recommandations et les lignes directrices par ordre d'importance, et ne doit pas être confondue avec un ensemble d'exigences restrictives similaires à celles utilisées dans les normes classiques (par exemple, ISO). Afin de fournir au groupe cible des indications claires, précises et sans ambiguïté sur ce qui est conforme ou non aux meilleures pratiques, la présente terminologie est utilisée.

C.1.2 Influence du contrôle électronique sur le processus d'authentification

Bien que l'accent soit mis sur la partie optique de l'authentification des DVLM, la partie électronique doit être prise en considération. Selon l'état actuel de la technologie, l'interaction entre une puce (DVLMe) et un module RF (lecteur de pages complètes) pendant le processus d'authentification est hautement probable et peut être attendue. Certaines des recommandations formulées dans ce document sont mieux comprises si l'on garde à l'esprit que les contrôles optiques et électroniques (le cas échéant) sont des processus complémentaires qui convergent vers un résultat global.

Deux aspects de l'interaction entre les contrôles électroniques et optiques présentent un intérêt particulier : la comparaison des données optiques et électroniques, et les implications du contrôle de la présence d'une puce si celle-ci est attendue. Pour ces deux aspects, l'influence du contrôle électronique ne peut être négligée et est mise en évidence dans les recommandations correspondantes.

C.2 DÉFINITIONS

Dans la section suivante, une terminologie cohérente est introduite pour une utilisation ultérieure. Le processus d'inspection des DVLM est décrit de manière générale dans le § C.2.1 et en détail dans le § C.2.2. Le § C.1.2 traite de l'influence de la partie électronique du processus d'authentification.

C.2.1 Processus d'identification et de vérification des DVLM

La vérification de l'authenticité d'un document de voyage comprend la vérification des éléments de sécurité optique du document. Elle est réalisée par un système d'authentification[2] qui se compose des éléments suivants : un lecteur de pages complètes, un logiciel d'authentification[3], une base de données d'authentification et éventuellement une base de données de référence.

Le lecteur de pages complètes crée des images en taille réelle du document de voyage à vérifier sous différentes sources de lumière. Cet *ensemble de données* dites « réelles » (images du document en taille réelle)[4] est transféré au logiciel d'authentification par le lecteur de pages complètes.

Le logiciel d'authentification identifie généralement ce que l'on appelle le *modèle de document* du document en utilisant la ZLA et/ou des informations supplémentaires (par exemple, le modèle spécifique du document, la date d'émission, les éléments optiques spécifiques, etc.) en entrée. Un modèle de document couvre les séries de documents d'un pays/ d'une nation qui ont la même apparence optique.

Conformément à la directive technique BSI-TR-03135, un modèle de document est défini au moyen du code pays (C), du type de document (T), d'un numéro d'identification unique (N) et de la valeur de l'année de première émission (Y) :

Modèle de document : = (C, T, N, Y)[5]

Le code pays C doit être rempli selon les spécifications du Doc 9303 de l'OACI comme un code à trois lettres.

Le type de document T est également spécifié par l'OACI dans le Doc 9303.

Le numéro d'identification N doit être un numéro unique, chronologique et croissant, commençant par 1 et faisant référence au modèle – ou à la génération – du document.

L'année Y désigne l'année, sous la forme d'un nombre entier à 4 chiffres, au cours de laquelle un document de ce modèle particulier a été émis pour la première fois. Si l'année est inconnue, cette valeur doit être omise.

Par exemple, les deux modèles de passeport/document britannique de 2008 et de 2010 en circulation ont les identifiants suivants : (GBR, P, 1, 2008) et (GBR, P, 2, 2010).

Il existe plusieurs approches techniques pour identifier le modèle de document. L'acquisition de la ZLA est l'une d'entre elles (voir § C.4.3.2). Si la ZLA est utilisée mais ne suffit pas à déterminer sans ambiguïté le modèle de document, des paramètres supplémentaires du document (par exemple, des motifs) doivent être utilisés pour aider à restreindre les résultats de l'identification, en particulier lorsqu'il s'agit de plusieurs modèles de documents valides du même pays (par exemple, un passeport britannique)[6].

---

2. Un système d'authentification décrit la combinaison d'un lecteur de pages complètes, d'un logiciel d'authentification, comprenant une base de données d'authentification et éventuellement la base de données de référence des experts.
3. Le logiciel d'authentification reçoit l'ensemble des données réelles du lecteur de pages complètes. Il fournit plusieurs algorithmes d'authentification afin d'appliquer les routines de contrôle à l'ensemble des données réelles.
4. Ensemble de données réelles : L'image visuelle, IR et UV du document testé à vérifier avec le système de lecture. Ces photos sont utilisées pour l'inspection du document.
5. Le présent Appendice ne porte que sur la partie optique de l'authentification des documents par machine. Cela signifie que des documents qui sont optiquement identiques mais qui diffèrent au niveau des caractéristiques électroniques sont considérés comme appartenant au même modèle de document.
6. Certains pays, comme l'Australie, utilisent une lettre de série pour distinguer différents modèles ou séries de documents (par exemple, la série N). Bien que cette méthode puisse être suffisante au niveau national, elle n'est pas très efficace pour la classification internationale en raison du manque de normalisation. Par conséquent, le présent document suit les recommandations de la directive technique BSI-TR-03135, qui sont considérées comme plus adaptées à des fins de classification internationale.

Le logiciel d'authentification envoie l'identifiant du modèle de document à la base de données d'authentification où sont stockées les *routines de contrôle*. Ces routines de contrôle définissent les procédures de test qui doivent être appliquées à l'ensemble des données réelles de ce modèle de document de voyage particulier. Un ensemble spécifique de routines de contrôle, appelé *ensemble de données d'authentification*, est déterminé pour chaque modèle de document. Après la réception de l'identifiant du modèle de document, la base de données d'authentification envoie l'ensemble de données correspondant au logiciel d'authentification. De plus amples détails sur la configuration d'une base de données d'authentification sont fournis dans le § C.2.2. (Voir la Figure C-1.)

La vérification est ensuite effectuée par le logiciel d'authentification. Les routines de contrôle sont appliquées à l'ensemble des données réelles du document de voyage. Cet examen débouche généralement sur un résultat de type « réussite » ou « échec ». Un résultat « réussite » signifie que le document contrôlé ne présente aucune anomalie, tandis qu'un résultat « échec » signifie le contraire. Selon le scénario d'application, l'interprétation du résultat (réussite ou échec) relève de la responsabilité de l'opérateur.

Si un ensemble de données vivantes ne peut être attribué sans ambiguïté à un modèle de document particulier, un sous-ensemble de routines de contrôle peut être exécuté (de manière facultative). Ces routines de contrôle sont spécifiées indépendamment du modèle de document.

Afin d'assister l'opérateur dans une vérification manuelle, le logiciel d'authentification peut demander l'*ensemble de données* dites *de référence* à partir de la base de données de référence sur la base du modèle de document identifié. L'ensemble de données de référence contient les images sous exposition à la lumière visible (blanche), l'IR et l'UV du modèle de document ; il peut également inclure des images plus détaillées des parties du document ainsi que des descriptions textuelles supplémentaires. Toutefois, cette base de données dite de référence, également appelée *base de données experte* dans la pratique, n'est pas un élément obligatoire du système d'authentification proprement dit. Le processus d'identification et de vérification des documents est illustré dans la Figure C-1.

C.2.2 Configuration détaillée d'une base de données d'authentification

Dans la base de données d'authentification, un ensemble distinct de routines de contrôle est stocké pour chaque modèle de document. Par exemple, les routines de contrôle pour le modèle de document allemand de 2007 diffèrent des routines qui doivent être appliquées au modèle de document britannique de 2008.

Une routine de contrôle d'un ensemble désigne une spécification de test pour la propriété d'un dispositif de sécurité optique. Par exemple, la routine de contrôle 1 de la Figure C-2 vérifie si la photo est absorbante à la lumière visible. Dans ce cas, la photo est l'élément optique, dont on teste la propriété d'absorption à la lumière visible (voir source lumineuse 1 n routine de contrôle 1). La mise en œuvre de cette routine de contrôle est effectuée par un algorithme d'authentification fourni par le logiciel d'authentification (voir l'algorithme d'authentification 1 dans la routine de vérification 1). Dans ce cas, l'algorithme 1 est un algorithme d'authentification qui vérifie la luminosité de l'élément. En revanche, la routine de contrôle x de la Figure C-2 vérifie si l'encre est luminescente à la lumière UV dans la zone de la photo en utilisant l'algorithme de « contrôle de motif » (algorithme de vérification n du logiciel d'authentification de la Figure C-2). Cet exemple montre clairement qu'un élément de sécurité optique peut offrir des propriétés différentes sous différentes sources de lumière (voir la Figure C-3).

Conformément au règlement de l'UE établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage[7], ces contrôles peuvent être raisonnablement répartis en trois catégories : matériau, technique d'impression et personnalisation.

7. Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004.

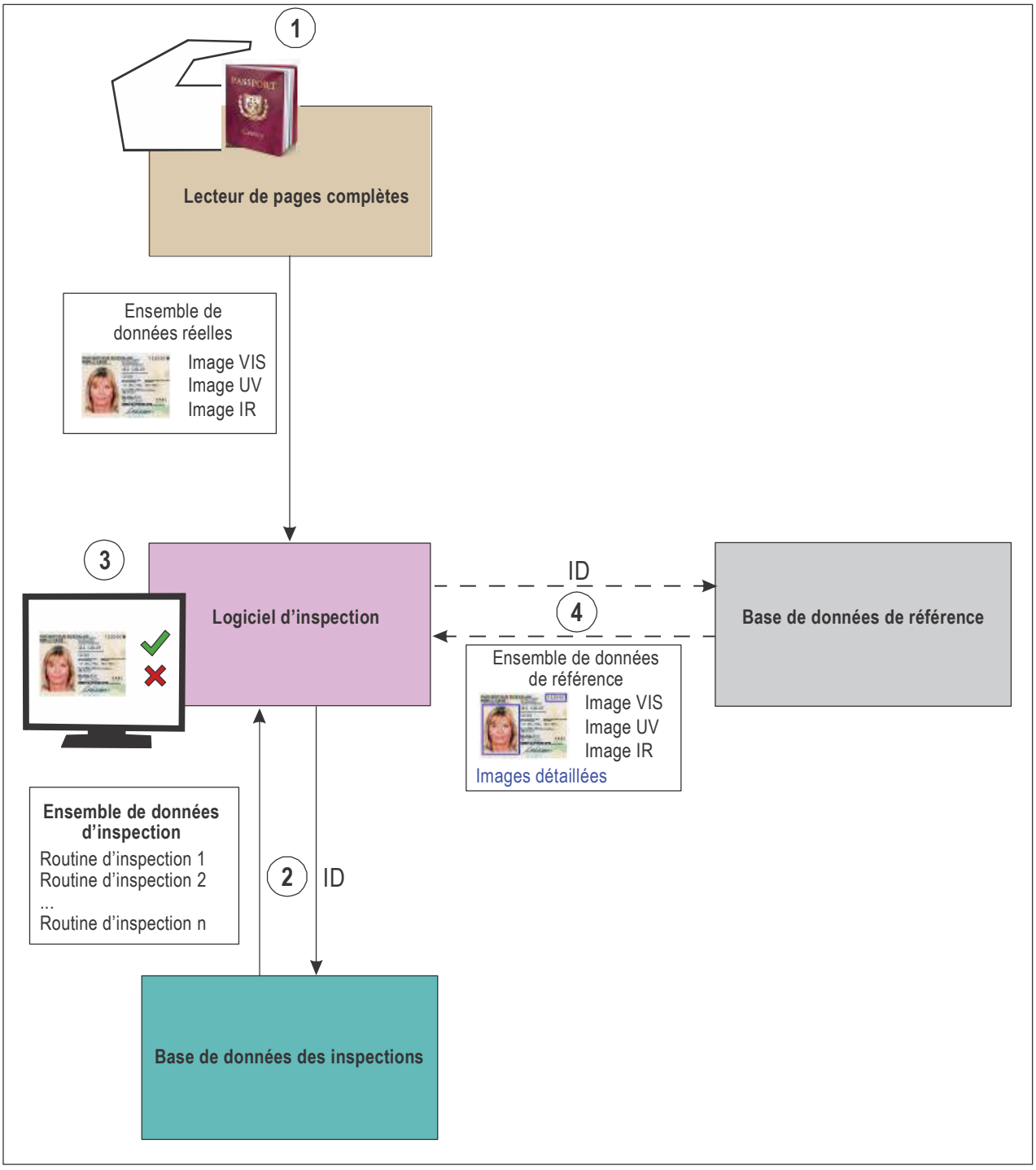

Figure C-1. Processus d'identification et de vérification des documents ; les chiffres indiquent l'ordre des étapes du processus concerné

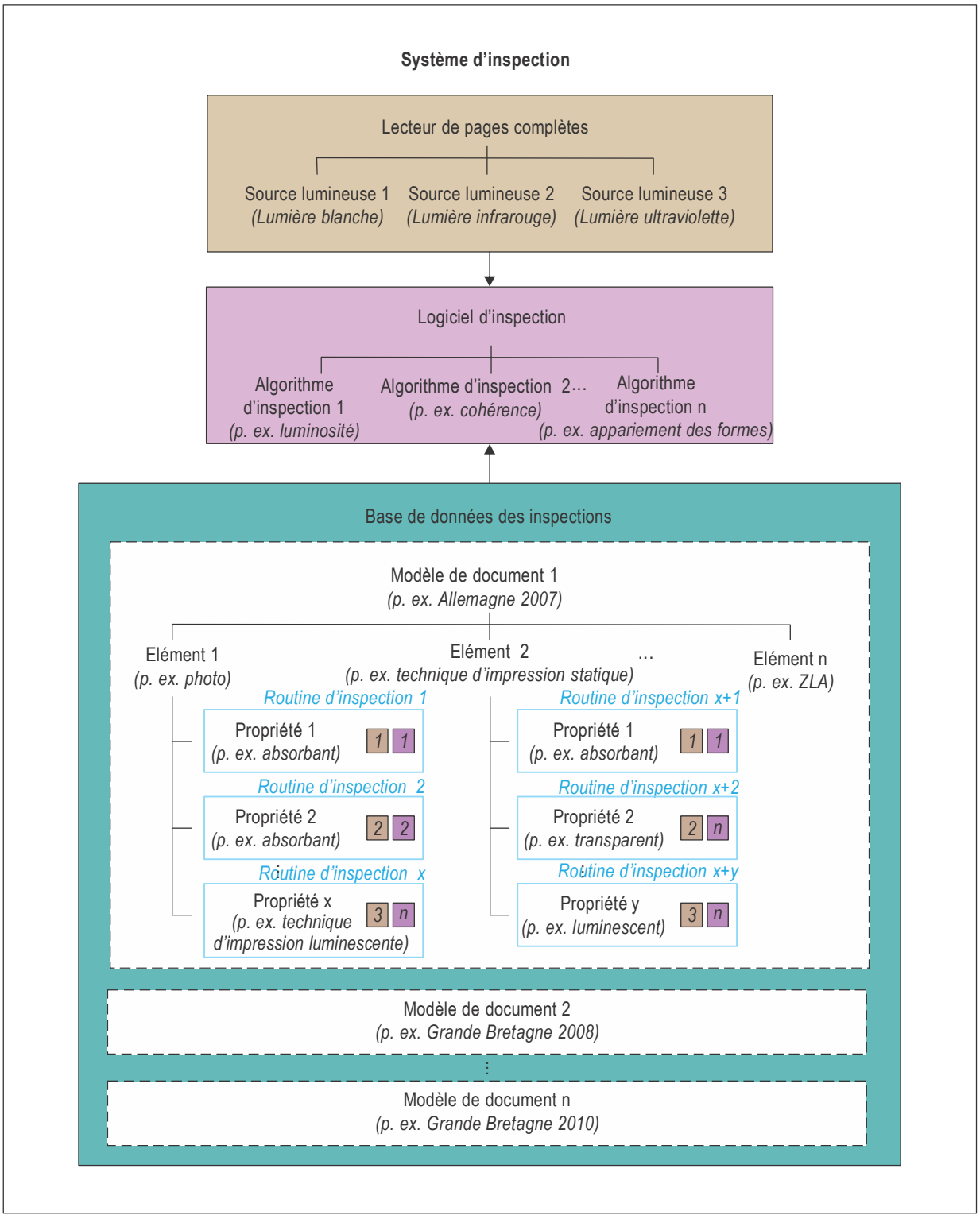

Figure C-2. Schéma de la mise en place d'un système d'authentification

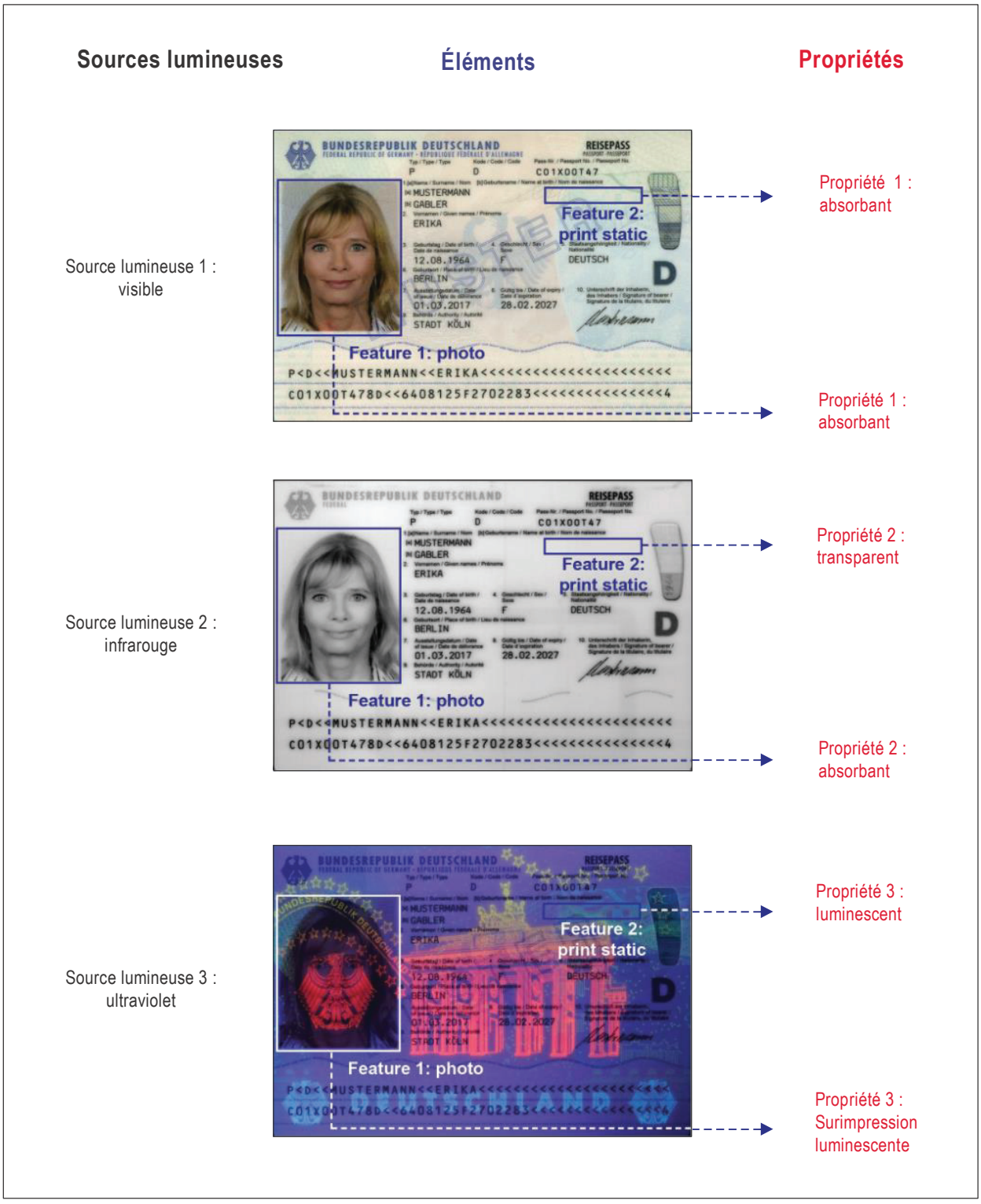

Figure C-3. Éléments et propriétés sous différentes sources de lumière en utilisant le passeport allemand

C.3 CATALOGUE DE ROUTINES DE CONTRÔLE GÉNÉRIQUES

Tous les développeurs d'un système d'authentification définissent leurs propres identifiants pour les routines de contrôle. Ces routines de contrôle sont distinctes pour chaque modèle de document ; cependant, les identifiants de ces routines de contrôle ne sont souvent pas explicites. Par conséquent, la comparabilité des routines de contrôle appliquées au même modèle de document pour différents systèmes d'authentification est, en général, inexistante.

Afin de résoudre ce problème, il est possible de définir un catalogue de routines de contrôle réalisables sur la base des éléments de sécurité spectralement sélectives des documents de voyage. Le contenu de ce catalogue pourra être étendu dans les futures versions de cette ligne directrice en conservant la nomenclature proposée. Les routines de contrôle correspondantes, dites spectralement sélectives, enregistrent les différentes réactions qui se produisent sur un document contrôlé sous exposition à la lumière visible (VI – lumière visible) ou extra visible (UV – ultraviolet, IR – infrarouge). Sur la base des trois enregistrements (VI, UV, IR), il est possible de vérifier les réactions d'absorption, de réflexion ou de luminescence de ces éléments. De manière séquentielle, ces routines de contrôle spectralement sélectives sont désignées par des routines de contrôle génériques telles qu'elles sont définies dans la directive technique BSI-TR-03135.

L'application de ce catalogue de routines de contrôle génériques améliorerait grandement la situation décrite ci-dessus et permettrait de mieux comprendre les mécanismes d'authentification par machine.

C.3.1 Description des routines de contrôle génériques

Les identifiants non ambigus (définis ci-dessous) des routines de contrôle ont été définis pour l'authentification par lecteur optique sur la base de la réaction spectrale des éléments de sécurité des documents de voyage. Ils peuvent être raisonnablement répartis dans les quatre catégories suivantes, définies dans l'Appendice A :

- Vérifier les propriétés du matériau (support) : Les réactions du support d'impression sont vérifiées, par exemple la luminosité sous la lumière UV.

- Vérifier les propriétés de la technique d'impression : Les éléments qui sont imprimés sur/dans le document, indépendamment de la personnalisation, sont testés, par exemple l'impression de formulaires.

- Vérifier les éléments qui empêchent de réaliser des copies : généralement des éléments diffractifs ou holographiques ou des laminés.

- Vérifier les propriétés de la technique d'émission (personnalisation) : Les éléments personnalisées sont testés, par exemple le nom du détenteur du document.

L'aspect optique des éléments de la catégorie « protection contre la copie » dépend beaucoup de la géométrie de l'éclairage. Par conséquent, les éléments de cette catégorie – qui se prêtent bien à l'inspection humaine – peuvent être très problématiques pour l'authentification par machine en général. C'est pourquoi les éléments de cette catégorie ne sont pas pris en compte par les routines de contrôle proposées.

Les 48 routines de contrôle génériques définies ci-dessous se composent de *routines de contrôle* dites *de base (RB)* et de *routines de contrôle composites (CR)*. Les routines de contrôle de base sont des routines individuelles, qui se réfèrent à une propriété (par exemple, l'absorption IR) d'un seul élément. Les routines de contrôle composites sont définies comme des combinaisons logiques de routines de contrôle de base. Par conséquent, un seul élément peut être testé pour de multiples propriétés telles que l'absorption IR et la transparence à la lumière visible.

Pour les routines de contrôle de base, les définitions abrégées suivantes, conformes à la directive technique BSI-TR-03135, sont utilisées :

Routine de contrôle de base : = (XX, YY, ZZ)

XX spécifie la source lumineuse de l'image sur laquelle la routine de contrôle est exécutée :

- **IR** – Lumière infrarouge
- **UV** – Lumière ultraviolette
- **VI** – Lumière visible (blanche)

YY est un identifiant pour la propriété optique de l'élément particulier :

- **AB** – absorbant, propriété de l'encre
- **BR** – brillance, propriété du support (par exemple, brillance sous exposition à la lumière UV)
- **FR** – propriété de fréquence spatiale des motifs (par exemple, caractéristiques des motifs obtenues après une transformation de fréquence spatiale, telle que la transformation spatiale de Fourier)
- **LU** – luminescent, propriété des motifs (par exemple, visible sous exposition à la lumière UV)
- **TL** – translucide, propriété de l'encre qui brille à travers le support
- **TR** – transparent, propriété de l'encre (par exemple, transparent sous exposition à la lumière IR)

ZZ est un identifiant[8] pour l'élément lui-même ou la position dans le document :

- **FI** – Fibres
- **FU** – Page de données (complète)
- **IS** – élément imprimé, qui existe déjà sur le support (encre statique)
- **MR** – Zone de lecture automatique (ZLA)
- **OM** – ZLA surimprimée
- **CA** – Numéro d'accès à la carte (abrégé : CAN)
- **BC** – Élément de code-barres

8. Dans cette nomenclature, les propriétés propres au modèle de document sont désignées comme « statiques » (comme la surimpression UV d'un blason), tandis que les propriétés propres au document (individuelles/personnalisées) sont désignées comme « dynamiques » (comme la surimpression UV répétant le numéro du document).

- **PD** – Perforation « dynamique » personnalisée
- **PS** – Perforation montrant un contenu « statique »
- **PH** – Zone de la photo
- **SP** – Zone de la photo secondaire
- **OP** – Photo surimprimée
- **TH** – Fil de sécurité
- **VZ** – Zone d'inspection visuelle (ZIV)
- **WM** – Filigrane
- **ID** – tout autre élément personnalisé « dynamique » (encre dynamique), par exemple, une photographie secondaire
- **AF** – tout autre élément supplémentaire qui ne peut être attribué aux éléments spécifiés ci-dessus

Si une routine de contrôle générique est constituée de plus d'une routine de contrôle unique, un numéro séquentiel doit être attribué à chaque routine de contrôle unique.

Les routines de contrôle génériques suivantes résultent de ces termes courts[9] :

Contrôle des propriétés des matériaux : (12 BR + 1 CR)

- **(IR, AB, PS)** → (IR, absorbant, perforation statique) : Vérifier si la perforation statique est visible sous la lumière IR.
- **(IR, AB, TH)** → (IR, absorbant, fil) : Vérifier si le fil de sécurité est visible sous la lumière IR.
- **(IR, AB, WM)** → (IR, absorbant, filigrane) : Vérifier si le filigrane est visible sous la lumière IR.
- **(UV, BR, FU)** → (UV, luminosité, complet) : Vérifier la luminosité de la page de données complète sous la lumière UV.
- **(UV, BR, MR)** → (UV, luminosité, ZLA) : Vérifier la luminosité de la ZLA sous la lumière UV.
- **(UV, BR, PH)** → (UV, luminosité, photo) : Vérifier la luminosité de la zone de la photo sous la lumière UV.
- **(UV, BR, VZ)** → (UV, luminosité, ZIV) : Vérifier la brillance de la zone d'inspection visuelle (ZIV) sous la lumière UV.
- **(UV, LU, FI)** → (UV, luminescent, fibres) : Vérifier la présence de fibres qui sont luminescentes sous la lumière UV.
- **(UV, LU, PS)** → (UV, luminescent, perforation statique) : Vérifier si les traces d'une perforation statique sont luminescentes sous la lumière UV.
- **(UV, LU, TH)** → (UV, luminescent, fil) : Vérifier la présence d'un fil de sécurité qui est luminescent sous la lumière UV.

9. Les routines de contrôle basées sur la fonction AF ne sont pas explicitement listées car elles peuvent être combinées avec chacune des sources lumineuses et propriétés optiques mentionnées.

- **(VI, TR, TH)** → (VI, transparent, fil) : Vérifier si le fil de sécurité est transparent à la lumière visible.

- **(VI, AB, PS)** → (VI, absorbant, perforation statique) : Vérifier si une perforation statique est visible à la lumière visible.

- **(IR, AB, TH)** ° (**VI, TR, TH)** → (IR, absorbant, fil) en combinaison avec (VI, transparent, fil) : Vérifier si un fil de sécurité, qui est visible sous la lumière IR, est transparent à la lumière visible.

Contrôle des propriétés de la technique d'impression : (8 BR + 2 CR)

- **(IR, AB, IS)** → (IR, absorbant, encre statique) : Vérifier si l'encre de l'impression statique est absorbante sous la lumière IR.

- **(IR, TL, IS)** → (IR, translucide, encre statique) : Vérifiez si l'encre au dos de la page de données (généralement la page de titre) est translucide sous la lumière IR et peut être détectée sur l'image IR de la page de données.

- **(IR, TR, IS)** → (IR, transparent, encre statique) : Vérifier si l'encre de l'impression statique est transparente sous la lumière IR.

- **(UV, LU, IS)** → (UV, luminescent, encre statique) : Vérifier si l'encre de l'impression statique est luminescente sous la lumière UV.

- **(UV, LU, OM)** → (UV, luminescent, ZLA surimprimée) : Vérifier si l'encre de l'impression statique est luminescente dans la ZLA sous la lumière UV.

- **(UV, LU, OP)** → (UV, luminescent, photo surimprimée) : Vérifier si l'encre de l'impression statique est luminescente dans la zone de la photo sous la lumière UV.

- **(VI, AB, IS)** → (VI, absorbant, encre statique) : Vérifier si l'encre de l'impression statique est absorbante à la lumière visible.

- **(VI, TR, IS)** → (VI, transparent, encre statique) : Vérifier si l'encre de l'impression statique est transparente à la lumière visible.

- **(IR, TR, IS)** ° **(IR, AB, IS)** → (IR, transparent, encre statique) en combinaison avec (IR, absorbant, encre statique) : Vérifier si certaines parties de l'impression statique sont absorbantes sous la lumière IR, alors que d'autres parties du même élément sont transparentes sous la lumière IR.

- **(IR, TR, IS) ° (VI, AB, IS)** → (IR, transparent, encre statique) en combinaison avec (VI, absorbant, encre statique) : Vérifier si l'encre de l'impression statique est à la fois transparente sous la lumière IR et absorbante à la lumière visible.

Vérification des propriétés de personnalisation : (28 BR + 3 CR)

- **(IR, AB, ID)** → (IR, absorbant, encre dynamique) : Vérifier si l'encre de l'impression dynamique est absorbante sous la lumière IR.

- **(IR, AB, MR)** → (IR, absorbant, contrôle B900 ZLA) : Vérifier si la ZLA est visible sous la lumière IR.

- **(IR, AB, CA)** → (IR, absorbant, CAN) : Vérifier si le CAN est visible sous la lumière IR.

- **(IR, AB, BC)** → (IR, absorbant, code-barres) : Vérifier si le code-barres est visible sous la lumière IR.
- **(IR, AB, PD)** → (IR, absorbant, perforation dynamique) : Vérifier si une perforation dynamique est visible sous la lumière IR.
- **(IR, AB, PH)** → (IR, absorbant, photo) : Vérifier si la photo est visible sous la lumière IR.
- **(IR, FR, PH)** → (IR, fréquence, photo) : Vérifier si le motif présente les caractéristiques attendues après la transformation de la fréquence spatiale.
- **(IR, AB, SP)** → (IR, absorbant, photo secondaire) : Vérifier si la photo secondaire est visible sous la lumière IR.
- **(IR, TR, SP)** → (IR, transparent, photo secondaire) : Vérifier si la photo secondaire est transparente sous la lumière IR.
- **(IR, TR, ID)** → (IR, transparent, encre dynamique) : Vérifier si l'encre de l'impression dynamique est transparente sous la lumière IR.
- **(IR, TR, PH)** → (IR, transparent, photo) : Vérifier la transparence de la photo sous la lumière IR.
- **(UV, FR, PH)** → (UV, fréquence, photo) : Vérifier si le motif présente les caractéristiques attendues après la transformation de la fréquence spatiale.
- **(UV, LU, SP)** → (UV, luminescent, photo secondaire) : Vérifier si la photo secondaire est luminescente sous la lumière UV.
- **(UV, LU, BC)** → (UV, luminescent, code-barres) : Vérifiez si le code-barres est luminescent sous la lumière UV.
- **(UV, LU, ID)** → (UV, luminescent, encre dynamique) : Vérifier si l'encre de l'impression dynamique est luminescente sous la lumière UV.
- **(UV, LU, PD)** → (UV, luminescent, perforation dynamique) : Vérifier si les marques d'une perforation dynamique sont luminescentes sous la lumière UV.
- **(VI, AB, ID)** → (VI, absorbant, encre dynamique) : Vérifier si l'encre de l'impression dynamique est visible à la lumière visible.
- **(VI, AB, MR)** → (VI, absorbant, ZLA) : Vérifier si la ZLA est visible à la lumière visible.
- **(VI, AB, CA)** → (VI, absorbant, CAN) : Vérifier si le CAN est visible à la lumière visible.
- **(VI, AB, BC)** → (VI, absorbant, code-barres) : Vérifier si le code-barres est visible à la lumière visible.
- **(VI, TR, BC)** → (VI, transparent, code-barres) : Vérifier si le code-barres est transparent à la lumière visible.
- **(VI, AB, PD)** → (VI, absorbant, perforation dynamique) : Vérifier si une perforation dynamique est visible à la lumière visible.
- **(VI, AB, PH)** → (VI, absorbant, photo) : Vérifier si la photo est visible à la lumière visible.
- **(VI, AB, SP)** → (VI, absorbant, photo secondaire) : Vérifier si la photo secondaire est visible à la lumière visible.

- **(VI, TR, SP)** → (VI, transparent, photo secondaire) : Vérifier si la photo secondaire est transparente à la lumière visible.

- **(VI, FR, PH)** → (VI, fréquence, photo) : Vérifier si le motif présente les caractéristiques attendues après la transformation de la fréquence spatiale.

- **(VI, AB, SP)** → (VI, absorbant, photo secondaire) : Vérifier si la photo secondaire est visible à la lumière visible.

- **(VI, TR, ID)** → (VI, transparent, encre dynamique) : Vérifier si l'encre de l'impression dynamique est transparente à la lumière visible.

- **(IR, TR, ID) (VI, AB, ID)** → (IR, transparent, encre dynamique) en combinaison avec (VI, absorbant, encre dynamique) : Vérifier si l'encre de l'impression dynamique est transparente sous la lumière IR et absorbante à la lumière visible.

- **(IR, TR, SP) ° (VI, AB, SP)** → (IR, transparent, photo secondaire) en combinaison avec (VI, absorbant, photo secondaire) : Vérifiez si la photo secondaire est transparente sous la lumière IR ainsi qu'absorbante à la lumière visible.

- **(VI, TR, BC) ° (IR, AB, BC)** → (VI, transparent, code-barres) en combinaison avec (IR, absorbant, code-barres) : Vérifier si le code-barres est transparent à la lumière visible et absorbant sous la lumière IR.

La routine de contrôle composite suivante est définie conjointement pour les deux classes de contrôle – impression et personnalisation :

- **(IR, TR, IS) ° (VI, AB, IS) ° (IR, AB, ID)** → (IR, transparent, encre statique) en combinaison avec (VI, absorbant, encre statique) en combinaison avec (IR, absorbant, encre dynamique) : Vérifier si l'encre de l'impression statique est à la fois absorbante à la lumière visible et transparente sous la lumière IR. En outre, un élément imprimé de manière dynamique est visible sous la lumière IR à la même position.

Les routines de contrôle spécifiées ci-dessus n'ont pas la même valeur par rapport à leur signification d'inspection. Par exemple, le résultat de la routine de contrôle (VI, AB, ID) n'est pas significatif en soi. Cependant, elle prend une importance cruciale pour la détection des contrefaçons lorsqu'elle est combinée avec la routine de contrôle (IR, TR, ID).

Les propriétés ou éléments propres à la contrefaçon doivent être incorporés en inversant la logique des routines de contrôle : par exemple, une configuration spécifique de fibres de sécurité imitées doit être contrôlée pour vérifier l'absence de ce motif (c'est-à-dire VI, TR, IS).

Le Tableau C-1 donne un aperçu de la classification du système de routine de contrôle générique. Les trois composantes des identifiants des routines – élément, source lumineuse et propriété – sont regroupées dans une matrice. Le contenu des lignes, des colonnes et des cellules décrit une routine de contrôle de base générique. Les classes de contrôle attribuées sont marquées par les couleurs vert (matériau), bleu (technique d'impression) et jaune (personnalisation).

Tableau C-1. Représentation matricielle des routines de contrôle de base génériques. Les propriétés optiques sont abrégées comme suit : AB – absorbant, propriété de l'encre ; BR – luminosité, propriété du support ; FR – fréquence spatiale, propriété des motifs ; LU – luminescent, propriété des motifs ; TL – translucide, propriété de l'encre qui brille à travers le substrat ; TR – transparent, propriété de l'encre ; les classes de contrôle sont marquées par les couleurs : vert (matériau), bleu (technique d'impression) et jaune (personnalisation).

Élément		*Source lumineuse*		
		VI	*UV*	*IR*
Fibres	FI		LU	
Page de données complète	FU		BR	
Caractéristique imprimée statique	IS	{AB. TR}	LU	{AB, TR, TL}
ZLA	MR	AB	BR	AB
ZLA surimprimée	OM		LU	
CAN	CA	AB		AB
Code-barres	BC	{AB, TR}	LU	AB
Perforation personnalisée (dynamique)	PD	AB	LU	AB
Perforation sur le support (statique)	PS	AB	LU	AB
Photo	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Photo secondaire	SP	{AB, TR}	LU	{AB, TR}
Photo surimprimée	OP		LU	
Fil de sécurité	TH	TR	LU	AB
Zone d'inspection visuelle, ZIV	VZ		BR	
Filigrane	WM			AB
Fonction dynamique personnalisée	ID	{AB, TR}	LU	{AB, TR}
Élément supplémentaire	AF	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}

C.4 RECOMMANDATIONS POUR L'AUTHENTIFICATION PAR MACHINE DES DVLM

Les composants clés suivants participent au processus d'authentification automatique par machines : le document, le lecteur de pages complètes et le logiciel d'authentification (y compris la base de données d'authentification, voir § C.2.2). Cependant, ces composants sont souvent conçus/fabriqués sans tenir compte de leurs interdépendances, notamment en ce qui concerne la conception du document de sécurité. Afin de pouvoir réaliser une authentification optimale par machine, il est essentiel que ces composants interagissent parfaitement entre eux.

Dans les sections suivantes, des recommandations sont données pour une conception efficiente et efficace du document (voir § C.4.1), du lecteur de pages complètes (voir § C.4.2), du logiciel d'authentification (voir § C.4.3), de la base de données d'authentification (voir § C.4.4) et de la base de données de référence (voir § C.4.5). Dans le § C.4.6, les recommandations formulées dans les sections précédentes sont transposées en scénarios d'utilisation à titre d'exemple afin d'aider les responsables opérationnels[10] à planifier l'exploitation des systèmes d'authentification optique.

Lors de l'examen des recommandations pour les différents composants, il convient de respecter les différences dans les échelles de temps généralement utilisées lorsqu'il est question des changements à effectuer :

- Logiciel du système d'inspection : 1 à 12 mois
- Matériel du système d'inspection : 3 à 5 ans
- Document de sécurité : 10 à 20 ans (résultant d'une période de délivrance typique de 5 à 10 ans, et d'une période de validité de 5 à 10 ans)

C.4.1 Concepteurs de documents

Pour concevoir un document comportant des éléments optiques aussi sûrs que possible, l'inspection humaine ne doit pas être le seul objectif du concepteur du document. Les éléments de sécurité offerts par le document doivent également être applicables à l'authentification par machine. En plus de la conception de base des DVLM, conformément au Doc 9303 de l'OACI, les sections suivantes résument les éléments appropriés pour l'authentification par machine. En outre, les sections suivantes résument également les éléments qui, même s'ils présentent un intérêt pour l'inspection humaine, peuvent contrecarrer l'authentification par machine (voir § C.4.1.2). Ces éléments sont qualifiés de « potentiellement interférents » dans le contexte de l'authentification par machine. Les concepteurs de documents ne devraient pas être dissuadés d'inclure ces éléments dans un document et devraient envisager de les inclure tout en gardant à l'esprit leur éventuel incidence (négative) sur le processus d'authentification par machine.

C.4.1.1 Éléments appropriées pour l'authentification par machine

Les recommandations concernant les éléments appropriées pour l'authentification par machine sont énumérées ci-dessous. Ces éléments ont été sélectionnées parce qu'ils sont faciles à détecter sur les images VI, IR et UV, mais en même temps, ces caractéristiques augmentent considérablement l'effort de contrefaçon pour le faussaire.

A.1 **Définir des éléments d'identification non ambigus :** Certains pays ont l'habitude de publier des modèles de documents successifs dans un laps de temps relativement court afin d'améliorer les propriétés de sécurité de leurs DVLM. Les modèles de passeport britannique (GBR, P, 1, 2008) et (GBR, P, 2, 2010)

10. Responsable opérationnel : L'organisation responsable de l'administration et de la gestion de tous les processus liés au fonctionnement de l'infrastructure d'authentification. Le responsable opérationnel établit et maintient des canaux de communication avec les vendeurs/fabricants des produits utilisés dans le système d'authentification final.

sont de bons exemples de modèles de documents successifs. Il est donc nécessaire, au cours du processus de conception du document, de définir des éléments qui permettent d'identifier sans ambiguïté le modèle de document (par exemple, un code-barres[11] spécifique à un modèle de document).

A.2 **Définir les éléments sous les trois sources de lumière :** Bien que la capture d'images sous ces sources lumineuses soit une caractéristique standard des lecteurs de pages complètes, l'expérience sur le terrain a montré qu'il est très difficile pour les contrefacteurs de reproduire correctement des éléments qui semblent authentiques sous plus d'une de ces sources lumineuses. La définition des éléments optiques de sécurité sous les trois sources de lumière (VI, IR et UV) est par conséquent nécessaire pour augmenter considérablement l'effort requis pour la production de contrefaçons.

A.3 **Définir les éléments en trois catégories :** Une répartition équilibrée des éléments de sécurité dans les classes « matériau », « technique d'impression » et « personnalisation » augmente également l'effort de contrefaçon. Par conséquent, les éléments doivent être définis dans chaque classe, conformément au Doc 9303 de l'OACI.

A.4 **Définir les éléments des deux faces des cartes d'identité :** Les cartes d'identité de taille ID-1 peuvent être positionnées sur un lecteur de pages complètes sur les deux faces. Par conséquent, les concepteurs de documents doivent concevoir des cartes d'identité de taille ID-1 ayant des éléments d'identification et de vérification sur les deux faces afin de permettre une identification et une vérification indépendantes de la face de la carte.

A.5 **Définir les éléments réagissant différemment sous différentes sources de lumière :** Les éléments du document qui se comportent différemment sous différentes sources de lumière (voir la Figure C-4), contribuent à réduire considérablement la probabilité de succès des contrefacteurs dans la production de contrefaçons correctes. Pour l'authentification par machine, il est donc nécessaire d'utiliser des éléments dont la présence et/ou l'absence peuvent être contrôlées, en fonction de la source lumineuse correspondante [par exemple, les encres métamériques, également appelées « IR split » dans la Figure C-4, contrôlables par routine (IR, TR, IS) (VI, AB, IS)].

Figure C-4. Passeport (CZE, P, 1, 2011) : IR split dans le texte du titre

11. Cet exemple d'utilisation du code-barres n'est pas en contradiction avec les recommandations du Doc 9303, Parties 9 et 10, pour le stockage électronique des données biométriques.

Figure C-5. Passeport (GBR, P, 2, 2010) : Motif UV avec deux couleurs[12]

A.6 **Définir les éléments ayant des couleurs différentes sous la lumière UV :** Les éléments ayant des couleurs luminescentes différentes sous la lumière UV (voir la Figure C-5) rendent la reproduction de cette caractéristique plus compliquée et sont donc recommandés. Parallèlement, le schéma de couleurs de cet élément peut être vérifié lors de l'authentification par machine, en plus du simple contrôle de présence de cet élément. En outre, il est recommandé d'utiliser des couleurs qui diffèrent sensiblement par rapport à leurs coordonnées chromatiques afin de faciliter la distinction par les machines. Les propriétés de luminescence des encres concernées ont tendance à se dégrader, ce qui rend encore plus difficile une détection automatique fiable.

A.7 **Définir des motifs ayant un contenu individuel, par exemple une image secondaire de visage :** Il est recommandé de définir des motifs individuels dont on peut à la fois vérifier la propriété et les comparer avec le contenu dynamique déjà existant sur la page de données. Par exemple, une image secondaire du visage peut être comparée à l'image primaire du visage, et ces deux représentations peuvent avoir des propriétés spectrales identiques ou différentes. La liste des motifs suivants ayant des images faciales secondaires vise à illustrer cette recommandation, mais elle n'est pas complète et ne constitue pas une recommandation explicite pour ces éléments spécifiques :

a) Image faciale secondaire en tant que répétition plus petite de l'image faciale qui est visible à la lumière visible et transparente sous la lumière IR [vérifiable par (VI, AB, ID) ° (IR, TR, ID)].

b) Encre optiquement variable (OVI) et dispositifs d'image optiquement variable par diffraction (DOVID) qui sont personnalisés, par exemple par gravure ou ablation au laser (voir la Figure C-6). L'exemple d'élément représenté sur la Figure C-6 montre différentes couleurs sous différents angles de vue à la lumière visible (première et deuxième image) et une image faciale secondaire légèrement visible à la lumière transmise (troisième image). Sous la lumière IR, l'image secondaire du visage peut être clairement capturée et comparée à l'image faciale. Cet élément peut être vérifié par la routine de contrôle composite suivante : (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), ce qui constitue une triple combinaison.

12.. Source : http://edisontd.net/

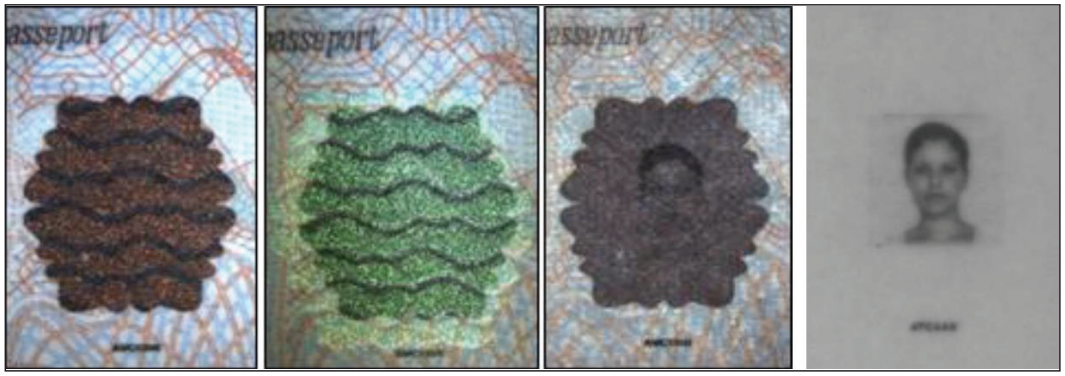

Figure C-6. Passeport (HUN, P, 1, 2006) : OVI personnalisée vue sous deux angles différents sous lumière transmise et sous lumière IR

c) Gravure laser personnalisée qui réagit de manière opposée (« négative ») (voir la Figure C-7). L'exemple d'élément présenté dans la Figure C-7 peut être capturé à la lumière visible, lorsqu'il montre une image faciale secondaire négative sous deux différents angles.

A.8 **Définir les éléments qui restent stables pendant la période de validité du DVLM :** Certains éléments ont tendance à s'user avec le temps. Les couleurs des motifs UV, par exemple, peuvent s'estomper pendant la période de validité du DVLM. Les colles de superposition peuvent faire perdre considérablement la netteté des motifs UV au fil du temps, ce qui peut entraîner des résultats de contrôle inexacts pour l'élément. Il est par conséquent recommandé de définir des éléments qui restent aussi stables que possible pendant la période de validité du DVLM.

Figure C-7. Passeport (LVA, P, 1, 2015) : Personnalisation « négative » par gravure laser sous différents angles d'observation à la lumière visible

A.8 **Définir les éléments qui restent stables pendant la période de validité du DVLM :** Certains éléments ont tendance à s'user avec le temps. Les couleurs des motifs UV, par exemple, peuvent s'estomper pendant la période de validité du DVLM. Les colles de superposition peuvent faire perdre considérablement la netteté des motifs UV au fil du temps, ce qui peut entraîner des résultats de contrôle inexacts pour l'élément. Il est par conséquent recommandé de définir des éléments qui restent aussi stables que possible pendant la période de validité du DVLM.

A.9 **Définir un porte-document utopien pour les spécimens de documents :** Afin d'établir un moyen normalisé d'identifier les spécimens de documents, il est recommandé de définir la nationalité du titulaire du document sur « UTO » pour les documents types.

C.4.1.2 Éléments potentiellement interférents pour l'authentification par machine

Cette section traite des éléments qui peuvent éventuellement interférer avec l'authentification par machine (dans le contexte mentionné au début du § C.4.1) :

- **Éléments superposés :** Les éléments superposés qui sont définis sans tenir compte de leur interdépendance peuvent interagir négativement sous l'influence d'une source lumineuse. Les effets de diffraction d'un DOVID peuvent interférer avec l'acquisition de la page de données (voir la Figure C-8).

- **Éléments à proximité du bord supérieur du document :** L'expérience sur le terrain a montré que les éléments optiques situés à proximité du bord supérieur du document (par exemple dans le cas d'un livret complexe) peuvent interférer avec l'authentification par machine et peuvent conduire à la coupure de la zone capturée. Une saisie partielle de cet élément pourrait entraîner des erreurs.

- **Éléments visibles uniquement en haute résolution :** En l'état actuel de la technologie, la plupart des lecteurs de pages complètes actuels utilisés dans les systèmes d'authentification supportent une résolution nominale maximale de 400 ppi et fournissent des résolutions optiques réelles qui sont même inférieures à cette valeur. Les éléments qui ne sont visibles qu'en haute résolution de plus de 400 ppi (par exemple, microtexte, guilloches) demeurent indétectables pour la plupart des lecteurs de pages complètes actuellement disponibles sur le marché (voir la Figure C-9). Toutefois, ces éléments pourront être vérifiées dans un avenir proche par des lecteurs de pages complètes affichant une résolution de 600 ppi ou plus.

- **Éléments dont l'apparence dépend de la manipulation individuelle :** Certains éléments ne sont potentiellement pas adaptés à l'authentification par machine car ils peuvent modifier considérablement l'apparence du document, c'est-à-dire que selon la façon dont la page est placée sur le lecteur de documents, le contenu de l'image réelle est plus ou moins différent. Deux de ces éléments sont mentionnés ci-dessous à titre d'exemple :

    a) *Élément de fenêtre : Selon la façon dont la page de données et la couverture sont placées sur le lecteur de documents,* il est possible de voir le contenu de la couverture à travers la fenêtre, le boîtier du lecteur, le bout du doigt ou le contenu de la fenêtre est vide (voir la Figure C-10), ce qui entraîne une lumière incidente.

    Une fenêtre unilatérale sur les cartes d'identité de taille ID-1, c'est-à-dire un élément de fenêtre qui ne peut être vu que de l'avant, convient mieux à l'authentification par machine car le contenu de la fenêtre ne varie pas dans la mesure de la Figure C-10 et n'entrave pas le processus de vérification au dos de la carte.

Figure C-8. Passeport (AUT, P, 1, 2006) : Film de sécurité à hologramme avec influence de distorsion optique

Figure C-9. Passeport (D, P, 1, 2017) : Comparaison entre une image à haute résolution du microtexte (1000 ppi) et une image du même microtexte prise à partir d'un lecteur de pages complètes (400 ppi nominal)

b) *Feuille de recouvrement transparente pleine page :* Ces feuilles peuvent donner des résultats différents selon leur présence (ou leur absence) pendant le processus de capture d'image (voir la Figure C-11).

Les difficultés liées à l'utilisation de ces éléments peuvent être surmontées par une formation adéquate de l'opérateur (dans le cas de l'inspection de documents assistée par l'homme) ou par des orientations pour l'utilisateur (par exemple pour le contrôle automatisé aux frontières).

- **Pages de visa supplémentaires :** Les passeports qui peuvent être modifiés par l'ajout de pages supplémentaires pour les visas peuvent devenir trop massifs pour les géométries ordinaires des lecteurs de pages complètes.

Figure C-10. Passeport (SWE, P, 1, 2012) : Élément de fenêtre à contenu variable ; de gauche à droite : couverture avant intérieure ; boîtier de lecteur ; bout du doigt ; éblouissement induit par la lumière incidente

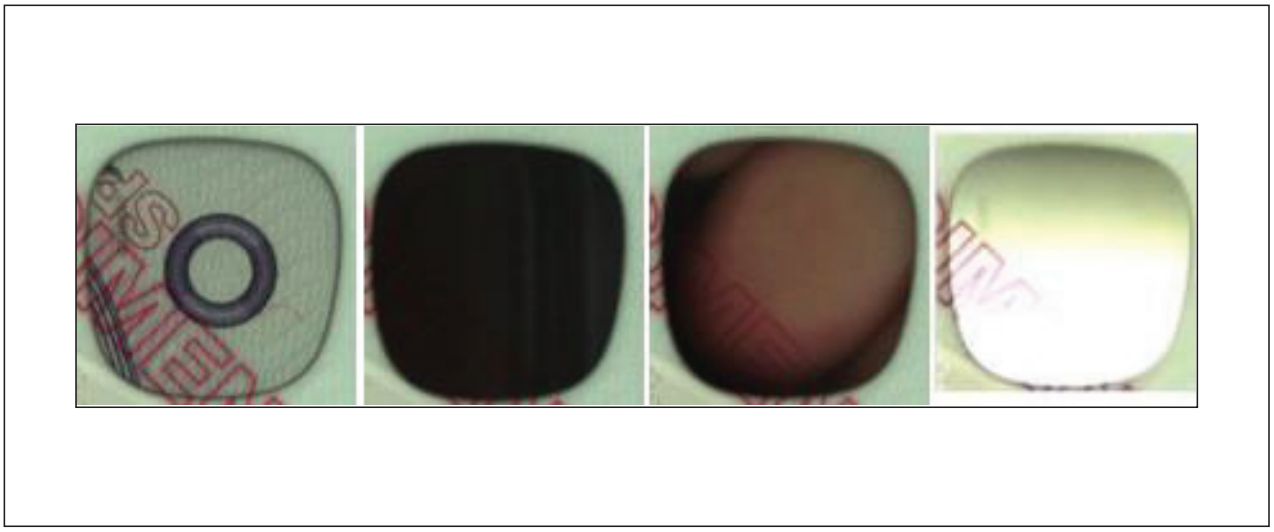

Figure C-11. Passeport (BEL, P, 1, 2008) ; à gauche : page de données simple ; à droite : page de données avec une superposition de la feuille transparente pour une inspection visuelle

C.4.2 Fabricant du lecteur de pages complètes

La fiabilité d'un processus d'authentification ne dépend pas seulement de l'ensemble des fonctionnalités fournies par le lecteur de pages complètes utilisé dans le processus ; une utilisation pratique et facile du lecteur de pages complètes déployé a également une incidence directe sur la qualité des images fournies au logiciel d'authentification (voir § C.4.3), et influence donc automatiquement le résultat global du processus d'authentification. Les recommandations génériques données dans la présente section doivent être prises en compte dans le processus de conception des lecteurs de pages complètes :

B.1 **Assurer des longueurs d'onde appropriées du spectre lumineux :** L'enregistrement d'images à l'aide de longueurs d'onde appropriées est une condition préalable à l'analyse adéquate des éléments et propriétés optiques. Par exemple, un élément censé être transparent sous une lumière IR peut devenir visible sur une image IR si la capture est effectuée avec une longueur d'onde inappropriée du spectre lumineux correspondant. Cela peut conduire à des ensembles de données réelles erronés, et donc à une mauvaise interprétation des résultats du contrôle optique. Les longueurs d'onde suivantes pour les spectres lumineux correspondants sont nécessaires pour enregistrer les images des ensembles de données réelles :

- VI : gamme spectrale de 400-700 nm
- IR : longueur d'onde comprise entre 850 et 950 nm[13]
- UV : 365 nm

Même si certains lecteurs de passeport prennent en charge des longueurs d'onde UV plus courtes (par exemple 254 et 313 nm), cette technologie n'est pas encore très répandue et n'est pas prise en compte dans le présent document.

B.2 **Assurer une résolution minimale :** La qualité des ensembles de données réelles fournis au logiciel d'authentification, mesurée en pixels par pouce (en abrégé : ppi), a une incidence directe sur la précision du processus d'authentification. L'expérience sur le terrain a montré que les ensembles de données réelles doivent avoir une résolution minimale de 385 ppi (BSI-TR-03135), bien que de nombreuses propriétés de l'impression de sécurité bénéficieraient d'une résolution d'acquisition de 600 ppi ou plus.

B.3 **Fournir des formats d'image standard :** Les ensembles de données réelles sont fournis dans les formats les plus largement utilisés/supportés. À titre d'exemple, les formats suivants peuvent être utilisés : BMP, JPG (y compris JPG2000) et PNG.

B.4 **Capture jusqu'à la taille ID-3 :** Le lecteur de pages complètes doit permettre la vérification des DVLM de toutes les tailles spécifiées dans le Doc 9303. La zone de capture devrait donc être adaptée aux documents jusqu'au format ID-3. Bien que le présent document se concentre sur les lecteurs de page complètes, il convient de garder à l'esprit qu'il existe des scénarios d'application qui ne nécessitent pas la vérification de DVLM de toutes tailles, mais qui exigent seulement que le lecteur de pages complètes numérise des documents d'une taille spécifique (par exemple, les dispositifs mobiles).

B.5 **Assurer la capture de toutes les zones avec la même qualité :** Le lecteur de pages complètes doit être capable de capturer la totalité de la page de données avec une qualité d'image constante. Cela peut, par exemple, être assuré par un éclairage homogène de la surface de capture.

13. Cette valeur a été tirée des recommandations définies dans le Doc 9303, Partie 3.

B.6 **Assurer un temps de réponse court et une intensité constante :** La source lumineuse utilisée pour la capture doit avoir un temps de réponse court et fournir une intensité lumineuse constante, car toute détérioration de la lumière au cours du processus d'authentification pourrait conduire à la génération d'ensembles de données réelles inadaptés.

B.7 **Assurer une qualité d'image constante :** Les sources lumineuses des lecteurs de pages complètes du même type peuvent émettre de la lumière différemment en raison des écarts liés à la production. De plus, ces conditions de source lumineuse d'un lecteur de pages complètes peuvent changer d'intensité au fil du temps. Le lecteur de pages complètes doit donc mettre en œuvre des fonctionnalités qui permettent de compenser les écarts, offrant ainsi une qualité d'image constante dans le temps et quel que soit le dispositif individuel utilisé. Deux exemples sont donnés ci-dessous afin d'illustrer comment cette recommandation peut être satisfaite :

a) Le fabricant fournit des fonctionnalités permettant d'effectuer la gestion des couleurs et un calibrage supplémentaire (par exemple, au moyen d'une carte de calibrage) et de personnaliser les paramètres du lecteur de pages complètes (par exemple, la luminosité, le temps d'exposition).

b) Le fabricant fournit des capteurs intégrés permettant la compensation automatique des écarts.

B.8 **Permettre le réglage de l'exposition à la lumière UV par le logiciel d'authentification :** Les différents modèles de documents nécessitent souvent une exposition différente à la lumière UV afin d'éclairer le document de manière optimale. Dans ce cas, les informations relatives à l'exposition à la lumière UV sont stockées dans la base de données d'authentification. Par conséquent, le lecteur de pages complètes doit permettre le réglage de l'exposition à la lumière UV via le logiciel d'authentification grâce à la transmission des paramètres UV stockés dans la base de données d'authentification (voir § C.4.4.2, point D.8.).

B.9 **Permettre la capture de plusieurs images UV :** Le lecteur de pages complètes doit prendre en charge plusieurs images capturées avec des paramètres d'exposition différents, par exemple pour une combinaison d'éléments UV présentant un fort contraste de luminescence (par exemple, une gamme dynamique élevée).

B.10 **Permettre des images sans éblouissement :** Des reflets peuvent apparaître sur l'image capturée et recouvrent souvent des données biographiques ou des éléments de sécurité de la page de données. Par conséquent, les images fournies par le lecteur de pages complètes doivent contenir le moins d'éclat possible. Cela peut être réalisé en capturant plusieurs images à la lumière visible (blanche) sous différents angles ou en utilisant un éclairage diffus.

B.11 **Fournir un mécanisme permettant de presser le document à plat sur la zone de capture :** Comme indiqué précédemment, la convivialité du lecteur de pages complètes influence directement l'efficacité et la rapidité du processus d'authentification. Le lecteur de pages complètes doit donc prévoir des mécanismes permettant de presser mécaniquement le document à plat sur la fenêtre afin de permettre une capture correcte des pages du document.

B.12 **Permettre une utilisation à une seule main :** En outre, le lecteur doit pouvoir être utilisé par une seule main et le processus de lecture doit être symétrique, de sorte qu'il puisse être utilisé par des droitiers et des gauchers.

B.13 **Fournir des orientations interactives aux utilisateurs :** Les orientations interactives pour les utilisateurs augmentent non seulement le confort d'utilisation du lecteur de documents, mais elles contribuent également à réduire considérablement la durée de l'ensemble du processus d'authentification. Les orientations interactives conçues pour l'utilisateur sont essentielles, en particulier pour les portes ABC qui suivent généralement une approche de libre-service : Contrairement au contrôle stationnaire des

documents, le matériel d'authentification des documents est utilisé par les détenteurs de documents eux-mêmes. Par conséquent, le lecteur de documents doit être capable de fournir des orientations interactives aux utilisateurs. Cela peut être réalisé, par exemple, en fournissant un flux en direct du document placé sur la surface de capture indiquant la progression de la capture d'image (par exemple, la métaphore du scanner). De cette manière, l'utilisateur reçoit un retour d'information direct et peut remarquer beaucoup plus rapidement si le document est placé correctement sur le lecteur de documents.

B.14 **Fournir du matériel ayant un degré élevé de robustesse :** Selon le scénario de déploiement, les lecteurs de pages complètes sont soumis à diverses conditions externes (mauvaise manipulation, humidité, etc.). Au fil du temps, ces conditions externes peuvent plus ou moins endommager les composants clés (par exemple, des rayures sur la surface de capture) du lecteur de pages complètes, accélérant ainsi l'usure, voire la rupture du dispositif. Il est donc recommandé d'équiper le lecteur de pages complètes de composants matériels robustes.

C.4.3 Fabricant de logiciels d'authentification

Les propositions suivantes sont basées, à titre d'exemple, sur la directive technique BSI-TR-03135 de l'Office fédéral allemand de la sécurité de l'information (BSI), car elle constitue actuellement la seule solution du secteur public dans ce domaine. Il est fortement recommandé de mettre en œuvre le logiciel d'authentification conformément à cette directive. Les recommandations suivantes doivent être comprises comme une extension de la directive technique BSI-TR-03135.

Veuillez tenir compte des recommandations techniques suivantes pour le logiciel d'authentification :

C.1 **Permettre le traitement d'images préenregistrées :** Le logiciel d'authentification doit aussi fonctionner sans matériel et doit pouvoir traiter des images préenregistrées (les exigences minimales pour les images sont présentées au § C.4.2, points B.1, B.2 et B.3). Cette fonctionnalité est particulièrement importante pour les processus d'évaluation automatisés. Cependant, il est nécessaire d'empêcher le logiciel d'authentification de traiter des images préenregistrées pendant le fonctionnement normal, car cela peut être utilisé comme un vecteur d'attaque potentiel. Par conséquent, l'utilisation de l'interface utilisée pour traiter les images préenregistrées doit être limitée à des configurations spécifiques (par exemple, la configuration de l'évaluation).

C.2 **Permettre le traitement d'images provenant de différentes sources matérielles :** Le logiciel doit être capable de traiter des images prises à partir d'au moins deux lecteurs de pages complètes différents sans dégradation des résultats de la vérification. Le fabricant du logiciel d'authentification doit donc fournir une spécification décrivant les propriétés des images fournies au logiciel d'authentification (espace couleur, contraste, etc.).

C.3 **Abstraire l'interface utilisateur graphique (GUI) du logiciel et du matériel d'authentification** : Le processus d'authentification optique d'un DVLM est, la plupart du temps, accompagné de la vérification électronique du DVLM et d'une vérification biométrique avec le visage du détenteur du document et éventuellement l'empreinte digitale. En outre, des vérifications des antécédents, par exemple auprès du système d'information Schengen (SIS), doivent être effectuées. Il est donc recommandé d'utiliser une couche d'abstraction entre l'interface utilisateur graphique et les composants logiciels et matériels concrets nécessaires aux vérifications des documents, des données biométriques et des antécédents. De cette façon, l'interface utilisateur graphique est indépendante de ces composants. En outre, les composants mentionnés peuvent être facilement changés sans modifier l'interface utilisateur graphique.

Dans les sections suivantes, les recommandations destinées aux fabricants de logiciels d'authentification sont structurées en fonction des étapes exécutées au cours du processus d'authentification. Le document doit être détecté

(voir § C.4.3.1), identifié (voir § C.4.3.2) et vérifié ultérieurement (voir § C.4.3.3). En outre, l'ensemble du processus doit être visualisé (voir § C.4.3.4) et documenté en utilisant des mécanismes de journalisation appropriés (voir § C.4.3.5).

C.4.3.1 Détection des documents

Pour la détection des documents placés sur la surface du lecteur, les recommandations suivantes sont données :

C.4 **Détection automatique et manuelle des documents :** Le logiciel d'authentification doit fournir des mécanismes de déclenchement automatique et manuel de la détection des documents. Le déclenchement manuel est particulièrement crucial si la détection automatique des documents ne fonctionne pas correctement.

C.5 **Compenser la rotation et recadrer la page de données capturées en conséquence :** La capture d'images est lancée automatiquement après que la page complète de données personnelles a été placée sur la surface de capture. Le logiciel d'authentification doit être capable de compenser une éventuelle rotation et de réaligner l'image automatiquement. En outre, l'authentification doit recadrer la page de données capturées en conséquence pour un traitement ultérieur.

C.6 **Détecter le document en fonction de la présence optique :** La présence d'un document ne peut être détectée qu'en utilisant ses propriétés optiques. Le processus de détection doit être effectué par voie optique même si une puce éventuelle est absente ou fonctionne mal (voir § C.1.3).

C.4.3.2 Identification

Une condition préalable à la vérification des documents est l'identification correcte du modèle de document. Pour l'identification d'un ensemble de données réelles, les recommandations suivantes sont données :

C.7 **Identifier le modèle de document :** Il est nécessaire d'identifier le modèle de document, indépendamment des méthodes appliquées, pour autant que la méthode appliquée garantisse une identification correcte du modèle de document. Les méthodes les plus couramment utilisées pour l'identification des modèles de documents sont l'analyse de la ZLA (y compris l'analyse des motifs) ou l'analyse des motifs uniquement.

C.8 **Permettre une identification rapide via la ZLA :** Si la ZLA est utilisée comme entrée principale pour l'identification du modèle de document, le logiciel d'authentification doit mettre en œuvre des méthodes et des routines permettant un processus d'identification rapide. Deux exemples sont donnés ci-dessous afin d'illustrer comment cette recommandation peut être satisfaite :

a) Commencer par la capture de l'image IR afin d'extraire la ZLA et d'établir le modèle du document.

b) Comme la génération d'images en pleine résolution peut prendre du temps, une capture d'image IR rapide pour une analyse précoce de la ZLA peut être réalisée avec une résolution inférieure au minimum recommandé pour l'image IR utilisée à des fins d'identification.

C.9 **Prévoir une solution de repli si la ZLA n'est pas lisible sous la lumière IR :** Une identification non ambiguë du modèle de document devrait être possible par tous les moyens, pour autant que le document le permette. Même si la ZLA n'est pas lisible sous la lumière IR (non conforme à l'OACI), le document doit être identifié correctement. Le fabricant du logiciel doit donc prendre en charge des solutions de repli, comme l'exécution d'une reconnaissance optique de caractères dans l'image VI pour l'analyse de la ZLA, si celle-ci n'est pas imprimée avec une encre absorbant les IR.

C.10 **Fournir un modèle de document sans ambiguïté :** Le fabricant du logiciel doit fournir un lien sans ambiguïté vers le modèle de document afin de permettre l'accès à l'ensemble des données d'authentification de ce modèle de document dans la base de données d'authentification.

C.11 **Permettre l'identification partielle :** Le logiciel d'authentification doit permettre de configurer une identification partielle afin de réduire considérablement les taux de fausse identification et de non-identification. Néanmoins, l'évaluation de l'identification partielle requiert une interaction humaine et des connaissances spécifiques sur les DVLM pour sélectionner manuellement le modèle de document correct et ne convient donc pas à tous les scénarios, par exemple les portes ABC.

C.12 **Permettre l'identification manuelle :** Le système doit permettre un choix entièrement manuel du modèle de document – au lieu du processus automatique et/ou en annulant le choix de la machine – pour les cas où le processus d'identification automatique du système échoue. En outre, le système ne doit permettre une identification manuelle que si une identification partielle ne peut être effectuée. L'identification manuelle requiert une interaction humaine, des connaissances spécifiques sur les DVLM et ne convient donc pas à tous les scénarios (par exemple, elle n'est pas pratique pour ABC).

C.13 **Identifier les cartes d'identité sur les deux faces :** Les documents de format ID-1 sont spéciaux dans le sens où la ZLA ne figure pas sur la page des données personnelles (montrant l'image faciale). Toutefois, les cartes d'identité de taille ID-1 peuvent être positionnées sur un lecteur de pages complètes sur les deux faces. Par conséquent, les documents de format ID-1 doivent être identifiables sur les deux côtés du document (voir la recommandation A.4 du § C.4.1.1).

C.14 **Identifier les spécimens de documents :** Le logiciel d'authentification doit également identifier les documents types ou les spécimens de documents comme tels et en informer l'opérateur, sans interrompre le processus d'authentification (voir recommandation A.9 du § C.4.1.1).

Les recommandations pour la visualisation de la procédure d'identification dans l'interface utilisateur graphique se trouvent dans le § C.4.3.4.

C.4.3.3 Vérification

Des recommandations pour la vérification des documents sont données ci-dessous :

C.15 **Effectuer un nombre minimum de contrôles spectralement sélectifs :** Des routines de contrôle spectralement sélectives doivent être exécutées afin de vérifier les réactions d'absorption, de réflexion ou de luminescence de l'ensemble des données réelles. Même si un document n'a pas pu être identifié, les contrôles obligatoires suivants doivent être effectués :

a) (IR, AB, MR) : cette routine de contrôle, également connue sous le nom de test B900, peut être exécutée sans sélection d'un modèle de document ;

b) (UV, BR, FU) : avec certaines restrictions sur la précision, cette routine de contrôle peut également être effectuée sur des ensembles de données réelles non identifiées.

Si le modèle de document est identifié, les vérifications spectralement sélectives suivantes, complémentaires de celles susmentionnées (c'est-à-dire le contrôle de la propriété optiquement opposée), doivent être effectuées en plus :

c) (IR, TR, *ZZ*) : au moins une vérification portant sur la propriété complémentaire « transparent sous la lumière IR » par rapport à (IR, AB, MR) doit être effectuée ;

d) (UV, LU, ZZ) : au moins une vérification portant sur la propriété complémentaire « luminescent sous la lumière UV » par rapport à (UV, BR, FU) doit être effectuée.

C.16 **Effectuer une vérification de cohérence de la ZLA :** Outre le nombre minimal de vérifications spectralement sélectives, des vérifications de plausibilité (par exemple, erreurs dans la MRZ, code à 3 lettres de l'OACI) doivent être effectués avec tous les documents afin de garantir une sécurité minimale, y compris en cas de non-identification.

C.17 **Effectuer des vérifications dans toutes les catégories :** Le logiciel d'authentification doit effectuer des routines de contrôle dans les trois catégories (matériau, technique d'impression et technique d'émission) et couvrir les trois images de sources lumineuses (voir recommandation A.3 pour les concepteurs de documents au § C.4.1.1).

C.18 **Vérifier la présence de la puce :** Si l'on s'attend à l'existence d'une puce RF pour un modèle de document particulier, qui ne fonctionne pas ou semble ne pas exister, cela doit clairement susciter un avertissement en plus des résultats optiques (voir § C.1.3).

C.19 **Vérifier les motifs dynamiques :** Il est recommandé de fournir des algorithmes qui comparent des motifs dynamiques individuels (par exemple, photo, signature). Par exemple, l'image faciale pourrait être comparée à une image faciale secondaire située sur la page de données (voir la Figure C-12 et recommandation A.7 pour les concepteurs de documents au § C.4.1.1).

C.20 **Combiner les routines de contrôle si nécessaire :** Certaines caractéristiques peuvent être vérifiées par différentes routines de contrôle. Par exemple, des éléments se comportant différemment sous différentes sources lumineuses servent d'entrée pour des routines de contrôles séparées (voir recommandation A.5 pour les concepteurs de documents au § C.4.1.1). Il est donc recommandé de combiner les résultats de ces routines de contrôle de manière logique ou de combiner les scores de contrôle par une fonction de décision. Par exemple, une routine de contrôle composite peut toujours produire une décision de réussite, même si le score d'une routine de contrôle de base est légèrement inférieur à son seuil.

Figure C-12. Passeport (EST, P, 1, 2013) : Vérifier l'image faciale dans l'image à la lumière visible par rapport à celle imprimée avec de l'encre luminescente UV

C.21 **Effectuer des routines de contrôle redondantes sur plusieurs positions :** Pour les éléments qui apparaissent plus d'une fois sur le document, la routine de contrôle correspondante doit également être exécutée sur plusieurs positions de l'ensemble de données réelles. Par exemple, pour le modèle de document (D, P, 1, 2007) de la Figure C-13, le motif de l'aigle UV peut être vérifié sur plusieurs positions. Une routine de contrôle effectuée sur plusieurs positions est appelée routine de contrôle redondante.

Outre les apparences multiples d'un élément, certains éléments sont statistiquement plus sujets à la falsification que d'autres. Dans de nombreux cas, les contrefacteurs modifient, par exemple, la date d'expiration ou substituent l'image faciale. Il est donc recommandé d'exécuter de manière redondante les routines de contrôle capables de détecter les attaques sur ces éléments « sensibles ».

C.22 **Exécution de routines de contrôle redondantes sur plusieurs couleurs UV :** L'exécution de routines de contrôle redondantes est également recommandée pour les éléments UV, qui apparaissent en plusieurs couleurs sur le document (voir recommandation A.6 et Figure C-5 pour les concepteurs de documents au § C.4.1.1).

Figure C-13. Vérification des motifs redondants

C.23 **Reliez et vérifiez les deux pages d'une carte d'identité :** La numérisation d'une deuxième page est automatiquement liée à la numérisation précédente si les deux proviennent du même document d'identité. En outre, il est recommandé de vérifier les deux faces des documents de taille ID-1 afin d'obtenir un résultat de vérification global pour les deux faces et augmenter autant que possible le nombre d'éléments optiques utilisés pour l'authentification du document (voir recommandation A.4 pour les concepteurs de documents au § C.4.1.1).

C.24 **Permettre la vérification croisée des données personnelles sur plusieurs pages :** Les données personnelles du titulaire du document doivent être identiques, quelle que soit la page sur laquelle elles apparaissent. Par exemple, les données personnelles figurant sur la page de données d'un passeport sont censées être identiques aux données personnelles figurant sur un visa potentiellement existant. Il est par conséquent recommandé d'effectuer des contrôles croisés sur plusieurs faces si, par exemple, on s'attend à ce que les contenus personnalisés soient identiques/redondants.

C.25 **Effectuer des routines de contrôle en fonction de l'importance :** Il n'est pas toujours nécessaire ou utile d'exécuter toute une série de routines de contrôle simplement parce qu'il est techniquement possible de les appliquer à l'ensemble des données réelles. Une approche plus efficace serait d'évaluer la pertinence des contrôles en corrélation avec le processus de vérification. Certaines routines de contrôle sont davantage susceptibles de fournir des résultats utiles que d'autres, et de fournir des informations permettant une analyse plus précise des résultats de la vérification. Par conséquent :

a) les vérifications doivent être effectués par ordre de leur pertinence/importance et les résultats doivent être immédiatement affichés dans l'interface utilisateur graphique (voir Visualisation au § C.4.3.4) ;

b) les résultats des vérifications doivent pouvoir être combinés par des fonctions de décision différentes de la simple combinaison logique ET (c'est-à-dire en utilisant les résultats pondérés des contrôles). Les fonctions de décision doivent être enregistrées dans le catalogue XML (voir la recommandation C.46 pour l'enregistrement dans le § C.4.3.5).

C.26 **Prendre en considération l'écart de l'élément :** Les éléments de sécurité peuvent changer avec le temps en raison de l'usure du DVLM, par exemple, certaines couleurs UV peuvent se dégrader. Toutefois, ces éléments doivent être vérifiés avec une fiabilité constante pendant la période de validité du DVLM. Par conséquent, les tolérances des routines de contrôle doivent être prises en compte.

C.27 **Détecter les attaques génériques :** Outre la vérification pure et simple des propriétés des éléments du document, le logiciel d'authentification doit fournir des outils permettant de détecter les traces d'attaques génériques, telles que les « dommages au papier », les « marques de découpe », la « substitution de photos » ou les « plis du film de sécurité » si les conditions d'éclairage le permettent. Le schéma des routines de contrôle génériques peut également être appliqué aux contrôles permettant de détecter les contrefaçons.

Des recommandations pour la visualisation de la procédure de vérification dans l'interface utilisateur graphique sont présentées dans la section suivante.

C.4.3.4 Visualisation

La visualisation des résultats de l'authentification est le processus par lequel l'utilisateur du système d'authentification reçoit un retour visuel et des informations sur les résultats du processus d'authentification. La visualisation doit être réalisée sous la forme d'une interface utilisateur graphique (en abrégé : GUI).

L'interface graphique pour la visualisation des résultats des vérifications optiques ne doit fournir à l'utilisateur que les informations les plus pertinentes afin de pouvoir déterminer les irrégularités à première vue. Ces informations sont subdivisées ci-dessous en ce qu'il est convenu d'appeler la « zone de résumé du processus » (voir C.29), la « zone optique générale » (voir C.30) et des informations plus détaillées dans la « zone optique détaillée » (voir C.35).

Des recommandations pour choisir les informations admissibles et les présenter de manière compacte et minimaliste sont formulées ci-après :

C.28 **Afficher toutes les vérifications des documents dans une seule interface utilisateur graphique (GUI) :** L'interface utilisateur graphique peut faire partie intégrante du logiciel d'authentification fourni ou être fournie et exploitée dans une couche d'abstraction distincte. Indépendamment de cela, il est recommandé d'afficher tous les types de contrôle effectués (électroniques, biométriques, optiques et de fond) dans une seule GUI. Cela réduit considérablement l'effort de l'opérateur du système et facilite l'évaluation des résultats du contrôle grâce à une meilleure vue d'ensemble du processus. En outre, une attention particulière doit être accordée aux anomalies ou irrégularités qui se produisent (voir recommandations C.41 à C.45).

C.29 **Toujours montrer la *zone de résumé du processus* :** Cette zone doit montrer le résultat global de l'authentification optique et doit être affichée à l'utilisateur sur la page de démarrage (voir la Figure C-14 pour un exemple d'interface graphique de contrôle fixe aux frontières). Cette zone doit toujours être visible pour l'utilisateur, indépendamment des autres détails sélectionnés sur les résultats de vérification spécifiques. La zone de résumé du processus doit montrer un résultat global de l'authentification optique avec un symbole de feu de circulation. En outre, la zone doit afficher une image faciale recadrée de la page de données à côté de l'image faciale stockée sur la puce, si elle est présente.

C.30 **Affichage de la *zone optique générale* sur la page de démarrage :** Cette zone présente un aperçu des routines de contrôle optique et doit être affichée à l'opérateur sur la page de démarrage.

a) Cette zone doit contenir les informations suivantes (voir la Figure C-14) :

- L'image VI (lumière visible) du document par défaut. Le personnel de l'opérateur doit pouvoir changer l'image par défaut en IR ou UV, en fonction des exigences spécifiques.
- Les données personnelles du titulaire du document contenues dans ZLA : nom, prénom, date de naissance, sexe, nationalité et données facultatives.
- Les données du document : type de document, numéro de document, État émetteur ou organisation émettrice, date d'expiration et données facultatives.
- La ZLA extraite pour permettre la comparaison avec la ZLA imprimée sur le document.
- Un bouton permettant le déclenchement manuel du processus de lecture du document.
- Une image faciale recadrée de la page de données à côté de l'image faciale stockée sur la puce, si elle est présente (voir § C.1.3) pour permettre une détection facile de la substitution de la photo.

b) Il est également recommandé d'afficher les informations suivantes dans la zone optique générale :

- L'âge du titulaire du document ainsi que la période de validité restante. Cette information peut être reconnue plus facilement et plus rapidement par l'opérateur que les dates contenues dans la ZLA.

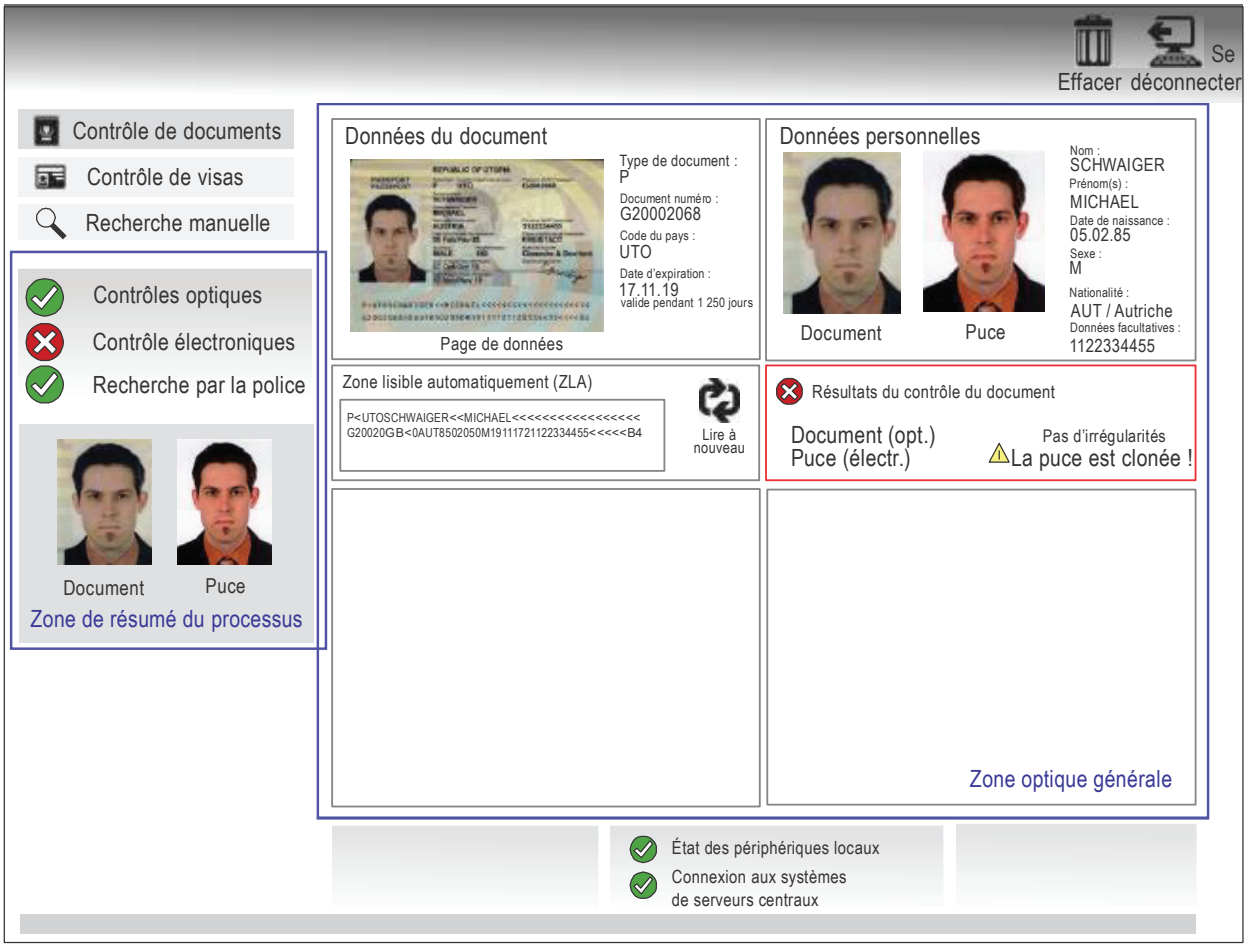

Figure C-14. Exemple de page de démarrage pour l'interface graphique de contrôle fixe aux frontières

C.31 **Sélectionner plus de détails en un seul clic** : À partir de la zone optique générale, l'opérateur doit cliquer une fois pour accéder à une page supplémentaire contenant davantage de précisions sur la vérification optique : la *zone optique détaillée* (voir C.35). Par exemple, dans l'exemple d'interface utilisateur graphique de la Figure C-14, il est possible d'obtenir plus de détails en cliquant sur la zone « Données du document ».

C.32 **Afficher les résultats avec les feux de circulation :** Comme spécifié dans la directive technique BSI-TR-03135, les résultats des processus de contrôle optique doivent être affichés à l'aide d'un système de feux de circulation (par exemple, feux rouges/verts/jaunes/gris). En plus de la couleur, les feux de signalisation doivent contenir des symboles non ambigus indiquant les résultats de la vérification (par exemple, une coche, une croix). Ceci est particulièrement important pour les utilisateurs atteints de daltonisme. En outre, le schéma de représentation doit être le même pour toutes les zones de l'interface graphique (par exemple, les résultats négatifs sont tous affichés avec le même symbole et la même couleur).

C.33 **Fournir la mise en correspondance des résultats conformément à BSI-TR-03135 :** Le système de feux tricolores doit fournir une correspondance cohérente avec les résultats de vérification suivants : **réussi**, **échoué**, **indéterminé** et **non pris en charge/non effectué**, définis dans BSI-TR-03135. Le Tableau C-2 donne un aperçu de la mise en correspondance utilisée dans ce document. Cette mise en correspondance est basée sur BSI-TR-03135 et doit être utilisée pour les mises en œuvre pratiques de l'interface utilisateur graphique.

C.34 **Fournir une mise en correspondance minimaliste des résultats :** Une autre solution consiste à utiliser une mise en correspondance minimaliste composée uniquement des couleurs verte et rouge pour le système de feux de signalisation. Comme le montre le Tableau C-3, la couleur verte peut être utilisée pour afficher un résultat de vérification positif, tandis que la couleur rouge peut être utilisée pour afficher tout autre résultat de vérification.

Une réduction supplémentaire de la mise en correspondance consisterait à afficher en rouge les quatre dernières vérifications dans les résultats du Tableau C-3.

Tableau C-2. Mise en correspondance du système de feux de circulation

Résultat de la vérification	*Couleur des feux de signalisation*
Réussi	vert
Échoué	rouge
Indéterminé	jaune
Non supporté/non réalisé	gris
Annulé	noir

Tableau C-3. Mise en correspondance minimaliste du système de feux de circulation

Résultat de la vérification	*Couleur des feux de signalisation*
Réussi	vert
Échoué	rouge
Indéterminé	
Non supporté/non réalisé	gris
Annulé	

C.35 **Afficher les détails dans une *zone optique détaillée* :** La vue détaillée n'est disponible que lors de l'extension de la zone et contient des informations détaillées sur les différents processus et résultats de l'authentification optique. Elle est destinée à fournir à l'utilisateur les informations nécessaires pour effectuer une analyse plus approfondie, si nécessaire.

a) La zone optique détaillée doit contenir les informations suivantes (voir l'exemple de la Figure C-15) :

- L'image VI, IR et UV du document. Les trois images doivent être présentées les unes à côté des autres.
- L'identifiant de modèle de document propriétaire du fabricant du logiciel d'authentification, si l'identifiant de modèle de document proposé au § C.2.1 ne peut être affiché sous forme générique.
- Une liste de routines de contrôle sélectionnées, montrant leurs résultats via des feux de signalisation : Dans le contexte du contrôle aux frontières, le garde-frontière ne doit être confronté qu'aux informations de vérification les plus importantes sous une forme lisible par l'homme. Par conséquent, les résultats des routines de contrôle génériques sont résumés en trois catégories, décrites par des termes faciles et compréhensibles, comme suit :
  - — Lisibilité IR de la ZLA : Le feu tricolore correspondant indique le résultat de la routine de contrôle générique (IR, AB, MR).
  - — Luminosité UV : Le feu tricolore correspondant indique le résultat combiné des routines de contrôle génériques (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) et (UV, BR, MR).
  - — Contrôle des motifs : Le feu tricolore correspondant indique le résultat combiné des autres routines de contrôle génériques qui ont été exécutées pour ce document (voir § C.3).
- En outre, les résultats des contrôles obligatoires suivants, conformément à la directive technique BSI-TR-03135, doivent être visualisés à l'aide de feux de circulation :
  - — Cohérence de la ZLA
  - — Date d'expiration
- La ZLA extraite.
- Au cours du processus d'authentification, les éléments de données extraits de la ZLA lue optiquement sont comparés aux éléments de la ZLA stockés sur la puce (si disponible). Les éléments de données de la ZLA optique doivent être affichés avec le ou les résultats de cette comparaison. Le ou les résultats doivent être affichés avec le même système de feux de circulation que celui utilisé dans l'interface graphique.

b) Il est également recommandé d'afficher les informations suivantes dans la zone optique détaillée :

- Le modèle de document identifié sous une forme lisible par l'homme, par exemple D 2007. L'utilisation de l'identifiant de modèle de document standard de BSI-TR-03135 pourrait probablement causer plus de confusion que de clarté parmi les utilisateurs de l'interface graphique. La représentation de l'identifiant du modèle de document dans l'interface graphique doit donc être spécifiée sur la base d'un accord commun avec l'opérateur du système d'authentification.
- Les éléments de données extraits de la ZLA lue optiquement et ceux extraits de la puce doivent être affichés les uns à côté des autres (voir § C.1.3).

Figure C-15. Exemple de vue de la zone optique détaillée

C.36 **Orienter les utilisateurs pendant la lecture des documents :** Au cours du processus de lecture, il convient de conseiller à l'utilisateur de ne pas retirer le document avant la fin du processus de lecture (voir recommandation B.13 au § C.4.2). Par exemple, cette indication peut être réalisée sous la forme d'un indicateur de processus affiché pendant le processus de lecture. Cette indication peut être placée dans la zone de résumé du processus.

C.37 **Afficher les informations des bases de données centrales :** Si le processus d'authentification requiert l'interrogation d'un système de base de données en arrière-plan, la page des détails optiques peut afficher les informations extraites de ce système si elles sont en corrélation avec l'authentification optique, par exemple l'image faciale extraite du système central d'information sur les visas (C-VIS).

C.38 **Prévoir une configuration homogène pour les DVLM :** La présentation de l'interface graphique doit être la même pour tous les types de documents lisibles par machine (par exemple, les passeports, les cartes d'identité nationales, les permis de séjour, etc.). Par exemple, les informations d'authentification optique obtenues des deux faces d'une carte ID-1 devraient être affichées de manière analogue à la visualisation

de la vérification du passeport (une zone de résumé du processus, une zone optique générale et une zone optique détaillée).

C.39 **Orienter les opérateurs dans la vérification de plusieurs pages :** La vérification des deux faces d'un document de format ID-1 exige des orientations interactives pour les utilisateurs. Pour une carte posée sur la surface de capture, l'utilisateur doit savoir que la présentation de la deuxième page pourrait être la prochaine étape.

C.40 **Permettre la comparaison du contenu du passeport et du visa/permis de séjour électronique :**

a) *Orienter les opérateurs dans la vérification de plusieurs pages* : Lors de la vérification d'un passeport, l'utilisateur doit être averti que le titulaire du passeport a besoin d'un visa/permis de séjour électronique pour franchir la frontière. Cela peut, par exemple, être réalisé par une incitation sur la page générale. Cette incitation doit indiquer à l'utilisateur que la présentation du visa/permis de séjour électronique au lecteur de pages complètes est une prochaine étape possible.

b) *Tenir à disposition les informations relatives au passeport :* Pendant l'authentification optique du visa/ permis de séjour électronique, les zones générale et détaillée et montrant les résultats de l'authentification du passeport doivent toujours être disponibles, afin de pouvoir passer à ces détails, si nécessaire.

c) *Permettre la comparaison dans la zone de résumé du processus :* Outre l'image faciale capturée optiquement sur la page de données, l'image faciale figurant sur le visa/permis de séjour électronique doit être affichée (voir l'exemple de la Figure C-16). En outre, l'image de la puce du titulaire du passeport (si elle est disponible, voir § C.1.3) et l'image extraite d'un système de recherche d'informations sur les visas (par exemple, le VIS européen) ou de la puce du permis de séjour électronique doivent être affichées (voir § C.37).

d) *Permettre la comparaison dans la zone optique détaillée du visa :* Au cours de la procédure d'authentification, les éléments de données Nom, Prénom, Date de naissance, Sexe et Nationalité extraits de la ZLA optique du visa sont comparés à ces éléments de la ZLA sur la page de données du passeport et/ou de la puce (voir § C.1.3). Les éléments de données de la ZLA du visa doivent être affichés avec le ou les résultats de cette comparaison. Le ou les résultats doivent être affichés avec le même système de feux de circulation que celui utilisé dans le reste de l'interface graphique. L'âge du titulaire du document ainsi que la période de validité restante du visa doivent également être affichés dans cette zone, car ces informations peuvent être reconnues plus facilement et plus rapidement par l'opérateur que les dates contenues dans la ZLA.

Des recommandations pour l'affichage des erreurs sont données ci-dessous :

C.41 **Ne surligner que les irrégularités :** Il est nécessaire d'utiliser le surlignage par la couleur uniquement pour signaler les irrégularités dans le processus d'authentification (par exemple, l'exemple d'échec de la vérification dans la Figure C-14). Cette approche aide considérablement l'utilisateur à reconnaître à première vue les informations les plus pertinentes fournies par l'interface graphique.

C.42 **Afficher les erreurs dans la zone de résumé du processus :** Si un document n'est pas authentique, le feu tricolore de l'authentification optique doit afficher un résultat global négatif. Si le modèle de document n'a pas pu être identifié, le feu tricolore du résultat global de l'authentification optique doit afficher un avertissement.

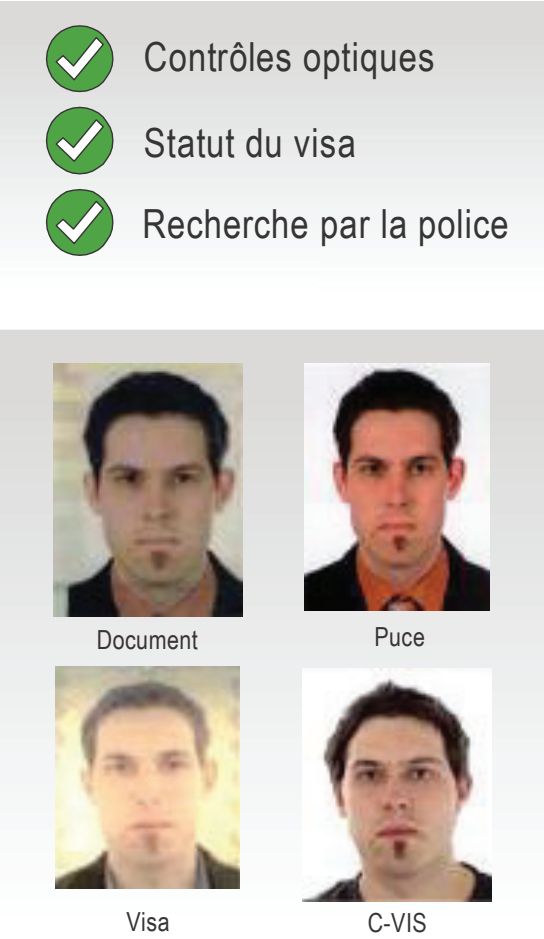

Figure C-16. Exemple de vue pour la comparaison du passeport et du visa

C.43 **Erreurs d'affichage dans la zone optique générale :** Si des erreurs se produisent en raison d'irrégularités optiques, elles doivent être affichées de la manière suivante :

a) *Irrégularité de la propriété spectralement sélective :* Si une erreur se produit à cause d'une routine de contrôle spectralement sélective, l'image du spectre lumineux correspondant doit être affichée dans la zone de données du document optique au lieu de l'image VI standard [par exemple, si (UV, BR, FU) échoue, l'image UV doit être affichée]. En outre, la zone optique générale doit être entourée d'un cadre rouge.

b) *ZLA non cohérente :* Si une erreur se produit à cause du contrôle de cohérence de la ZLA, la partie correspondante de la ZLA extraite, y compris la somme de contrôle, doit être surlignée en rouge. En outre, les données personnelles incohérentes correspondantes et la zone contenant les données personnelles doivent être surlignées en rouge (voir par exemple la Figure C-17). L'opérateur doit pouvoir corriger manuellement la ZLA et déclencher un autre processus de lecture à l'aide d'un bouton.

c) *Document expiré :* Si le document est périmé, la date d'expiration doit être mise en évidence en rouge.

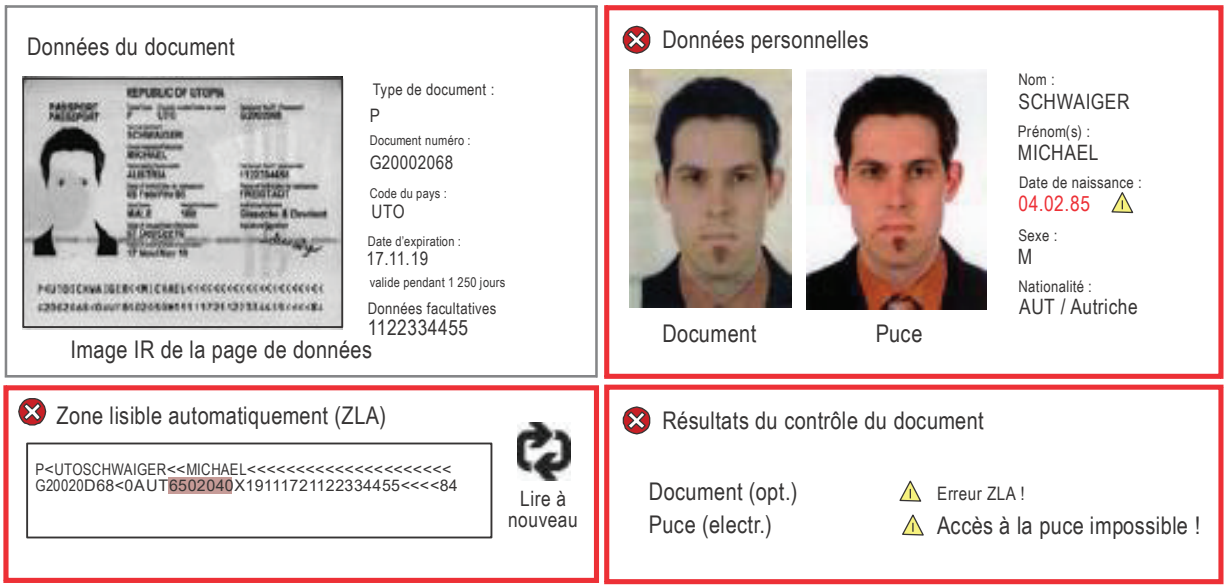

Figure C-17. Exemple de vue pour la visualisation des erreurs : Cohérence de la ZLA

d) *Puce non détectée :* Si une puce électronique est attendue dans le modèle de document identifié, mais qu'elle ne peut être détectée (voir § C.1.3), un avertissement doit être affiché. Le symbole d'avertissement doit pouvoir être clairement distingué des symboles de feux de circulation utilisés pour afficher les résultats du contrôle (par exemple, un panneau d'avertissement triangulaire jaune).

C.44 **Affichage des erreurs dans la zone optique détaillée :** Si des erreurs se produisent en raison d'irrégularités optiques, elles doivent être affichées de la manière suivante :

a) *Document non identifié :* Si le modèle de document n'a pas pu être identifié, un symbole d'avertissement doit être affiché comme résultat de l'identification du modèle de document. Le symbole d'avertissement doit pouvoir être clairement distingué des symboles de feux de circulation utilisés pour afficher les résultats du contrôle (par exemple, un panneau d'avertissement triangulaire jaune, voir Figure C-18). Un texte d'avertissement doit être affiché à côté du symbole d'avertissement, par exemple « Le modèle de document n'a pas pu être identifié ».

b) *Contrôle de vérification négatif :* Pour chaque contrôle de vérification affiché dans la page des détails (voir la Figure C-18), un résultat de contrôle négatif doit entraîner un feu rouge. Les caractéristiques respectives de l'échec du contrôle sélectif spectral doivent être surlignées sur l'image correspondante, par exemple en montrant un rectangle rouge entourant la zone de recherche de l'élément (par exemple, la ZLA de l'image IR en raison d'une lisibilité IR ZLA négative).

c) *Informations incohérentes sur la puce :* Pour chaque donnée ZLA qui n'est pas la même pour la page de données optiques et la puce (voir § C.1.3), la paire d'informations incohérentes doit être affichée en rouge (avec un symbole d'avertissement, voir Figure C-19).

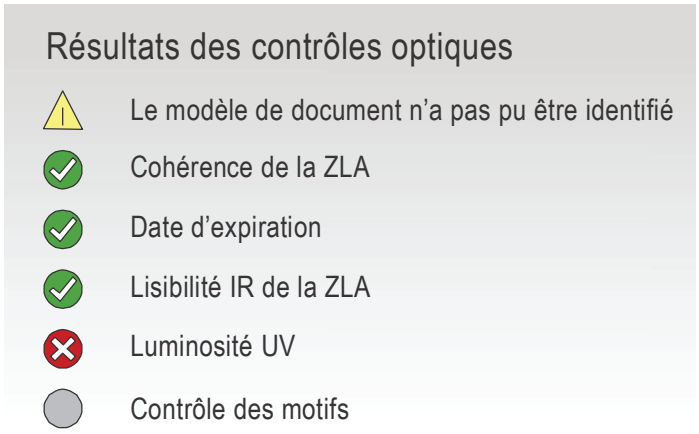

Figure C-18. Exemple de vue pour la visualisation des erreurs : Modèle de document et contrôle de vérification négatif

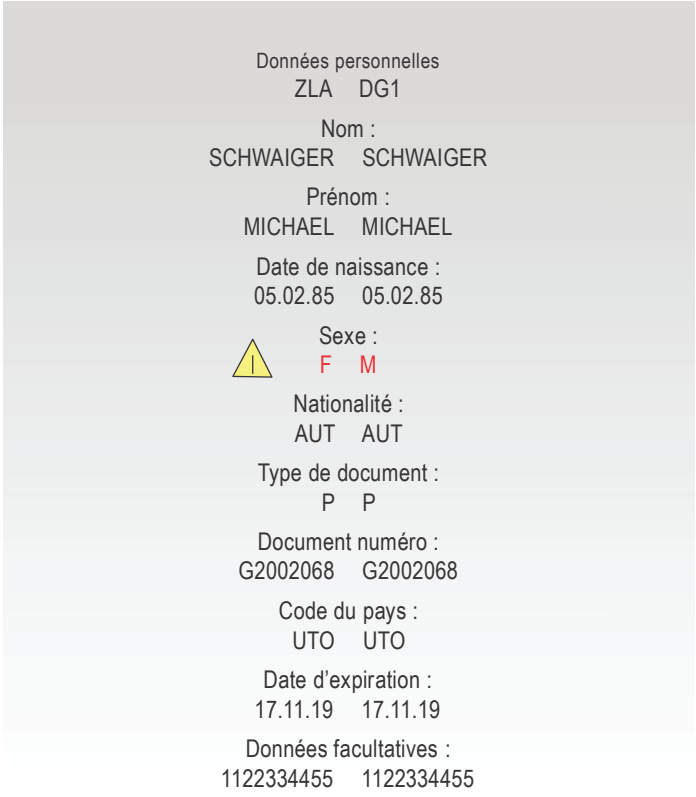

Figure C-19. Exemple de vue pour la visualisation des erreurs : Données de la ZLA

d) *Chiffre de contrôle global incohérent :* Les erreurs liées au chiffre de contrôle global [voir Doc 9303, Partie 3, Chapitre 4 (« ZLA »)] pourraient indiquer une manipulation des chiffres de contrôle, par exemple l'insertion de chiffres de contrôle incorrects dans la ZLA afin d'empêcher l'exécution de mécanismes de contrôle d'accès [par exemple, le contrôle d'accès de base (CAB)]. Pour chaque échec de contrôle sur la ZLA optique, le chiffre de contrôle saisi de l'élément de la ZLA correspondant doit être affiché à côté du chiffre de contrôle attendu.

C.45 **Erreurs d'affichage de la comparaison entre passeport et visa/permis de séjour électronique :** Si au moins une des données comparables de la ZLA n'est pas la même pour le passeport et le visa/permis de séjour électronique, cette incohérence doit être affichée de la manière suivante :

a) *Zone générale du visa/permis de séjour électronique :* Les données comparables de la ZLA (nom, prénom, date de naissance, sexe et nationalité) du passeport doivent être affichées dans la page générale du visa/permis de séjour électronique à côté des données du visa/permis de séjour électronique de la ZLA. Toute paire d'informations incohérentes doit être affichée en rouge avec un symbole d'avertissement (voir l'exemple de la Figure C-20).

b) *Zone détaillée du visa/permis de séjour électronique :* Pour chaque donnée de la ZLA qui n'est pas la même pour le visa/permis de séjour électronique et le passeport, la paire d'informations incohérentes doit être affichée en rouge (avec un symbole d'avertissement).

Figure C-20. Exemple de vue de la comparaison des données du visa et du passeport

C.4.3.5 Journalisation

Pour la journalisation du processus d'authentification par lecteur optique, les recommandations suivantes sont applicables :

C.46 **XML de journal selon BSI-TR-03135 :** La journalisation doit être réalisée selon les schémas XML définis dans BSI-TR-03135 qui contiennent également, outre les résultats optiques détaillés, les résultats de la vérification électronique et combinée (optique et électronique) d'un document. Par exemple, cela permet :

a) L'enregistrement de l'identifiant générique de routine de contrôle d'une routine de contrôle propriétaire (voir § C.3).

b) La mise des routines de contrôle en mode silencieux, c'est-à-dire que la routine est exécutée et ses résultats sont enregistrés, mais le résultat du contrôle n'est pas pris en compte dans le résultat global du processus d'authentification. Ceci est particulièrement important si de nouvelles routines de contrôle, de nouveaux algorithmes ou de nouveaux seuils sont évalués.

L'opérateur peut avoir besoin d'informations supplémentaires sur les contrôles spectralement sélectifs à des fins d'évaluation et pour mettre à jour la base de données sous-jacente afin de garantir des résultats d'authentification cohérents et de haute qualité dans le temps. Ces informations sont les mêmes pour tous les documents d'un modèle de document spécifique ; par exemple la fonction de décision, les explications textuelles sur les routines de contrôle et la section image de la base de données de référence. Par conséquent, le fabricant doit fournir ce catalogue XML sous une forme lisible par machine conformément au schéma XML défini dans BSI-TR-03135, qui résume toutes les informations nécessaires sur les vérifications spectralement sélectives. Grâce à son format, le catalogue peut être intégré dans l'évaluation des résultats.

C.47 **Permettre la journalisation de données d'image facultatives :** Les schémas XML définis dans la norme technique BSI-TR-03135 permettent, mais ne réglementent pas directement, le stockage de l'ensemble des données réelles traitées ainsi que des images recadrées affichant la zone de recherche des routines de contrôle. Le logiciel d'authentification doit être capable de stocker les données d'image mentionnées dans la structure de données XML. Des recommandations à l'intention du responsable opérationnel pour le stockage des données d'image conformément aux réglementations en vigueur en matière de protection des données sont formulées au point C.5.

C.48 **Fournir des capacités d'anonymisation :** Le logiciel doit permettre d'anonymiser l'ensemble des données réelles directement après l'authentification, afin de pouvoir stocker les images de manière permanente pour une inspection ultérieure. Veuillez vous reporter au § C.5.1 pour les recommandations concernant l'anonymisation.

C.4.4 Fabricant de la base de données d'authentification

Comme décrit dans les § C.2.1 et C.2.2, la base de données d'authentification contient des ensembles distincts de routines de contrôle pour différents modèles de documents. Il interagit directement avec le logiciel d'authentification auquel il fournit l'ensemble des routines de contrôle correspondant au modèle de document identifié. En raison des nouveaux modèles de documents établis et des contrefaçons qui apparaissent en permanence, une base de données d'authentification flexible et bien entretenue est cruciale. Dans les sections suivantes, les recommandations pour la base de données sont résumées concernant le processus de mise à jour (voir § C.4.4.1) et la configurabilité de la base de données (voir § C.4.4.2).

C.4.4.1 Mise à jour

Les recommandations suivantes sont données aux fabricants de bases de données d'authentification concernant le processus de mise à jour :

D.1 **Échanger des informations sur les nouveaux modèles de documents ou les contrefaçons :** Le fabricant de la base de données d'authentification établit un canal de communication spécifique avec le responsable opérationnel pour le transfert sécurisé des ensembles de données d'information sur les nouveaux modèles de documents qui doivent être insérés dans la base de données. Le fabricant échange des informations sur les nouveaux modèles de documents avec le responsable opérationnel en utilisant l'une des méthodes suivantes :

a) *Échange via l'échantillon original :* Dans ce cas, un échantillon original du nouveau modèle de document ou de la contrefaçon doit être fourni pour la définition et le téléchargement de l'ensemble correspondant de routines de contrôle dans la base de données. Le canal de communication établi et les processus associés doivent tenir compte de la législation nationale sur la protection des données (voir § C.5).

b) *Échange via un logiciel de capture :* Dans ce cas, un logiciel de capture doit être fourni au responsable opérationnel afin de générer un ensemble approprié de données réelles de nouveaux modèles de documents ou de contrefaçons. Cet ensemble de données doit contenir au moins une image VI, UV et IR. De préférence, plusieurs images d'un même spectre lumineux devraient être générées par ce logiciel de capture (par analogie avec la photographie à gamme dynamique élevée). L'ensemble de données est transféré au fabricant pour la définition d'un ensemble correspondant de routines de contrôle à inclure dans la prochaine édition de la base de données. Le fabricant doit recommander une liste de dispositifs de capture appropriés à cette fin.

D.2 **Mettre régulièrement à jour la base de données :** La base de données d'authentification doit permettre des mises à jour régulières (au minimum tous les trois mois). La base de données d'authentification doit également permettre des mises à jour ponctuelles sur demande spéciale (urgente) :

a) si le fabricant a obtenu de nouvelles informations sur les documents authentiques ou les contrefaçons et a mis à jour la base de données de documents sur la base de ces informations en coopération avec le responsable opérationnel (voir D.1 a), ou

b) si l'opérateur a généré un ensemble de données réelles avec le logiciel de capture (document authentique ou contrefaçon) et l'a envoyé au fabricant (voir D.1 b).

D.3 **Fournir des mises à jour progressives :** Par défaut, le fabricant de la base de données d'authentification doit fournir à l'opérateur les mises à jour de la version complète. Les mises à jour progressives devraient également être distribuées afin d'économiser du temps et de la bande passante.

D.4 **Fournir une documentation suffisante sur les changements :** Lors de la livraison de la mise à jour, le fabricant de la base de données d'authentification doit fournir une documentation suffisante sur les modifications apportées à la base de données.

C.4.4.2 Contenu et configurabilité de la base de données

La présente section présente une liste de recommandations pour les fabricants de bases de données d'authentification concernant le contenu et la configurabilité de la base de données :

D.5 **Fournir un contenu réduit :** La base de données d'authentification doit être disponible avec différentes portées et donc personnalisable pour différents scénarios. Par exemple, les scénarios commerciaux ont une portée limitée et le type de documents contrôlés est généralement très spécifique (par exemple, l'authentification de documents chez les entreprises de location de voitures). Il est par conséquent recommandé de fournir des bases de données d'authentification qui répondent spécifiquement aux besoins des scénarios commerciaux au moyen d'une complexité réduite. En proposant une base de données au contenu réduit, le fabricant s'assure qu'elle reste rentable et facile à intégrer dans différentes configurations.

D.6 **Attribuer des contrôles avec des niveaux d'importance :** Les contrôles doivent être affectés d'un niveau d'importance permettant au logiciel d'authentification d'effectuer les contrôles par ordre d'importance (voir la recommandation C.25 a) pour les fabricants de logiciels d'authentification visés au § C.4.3).

D.7 **Fournir différents modes opérationnels :** Différents scénarios d'utilisation exigent différents niveaux de sécurité concernant l'acceptation ou le rejet d'un document. Les contrôles fixes aux frontières, par exemple, reposent sur une sécurité élevée, tandis que les scénarios commerciaux sont davantage axés, en général, sur une grande commodité pour le détenteur du document. Par conséquent, la base de données d'authentification doit fournir au moins deux modes de fonctionnement différents pour une sécurité élevée et une grande commodité.

D.8 **Fournir des informations sur l'exposition aux UV propres au modèle de document :** Comme mentionné dans le § C.4.2, les différents modèles de documents nécessitent souvent une exposition différente à la lumière UV. Par exemple, certains modèles de documents nécessitent une illumination UV plus longue afin de vérifier correctement des caractéristiques spécifiques sous la lumière UV. Par conséquent, la base de données d'authentification doit contenir des informations sur les paramètres d'exposition aux UV requis pour les modèles de documents correspondants, afin que le logiciel d'authentification puisse configurer automatiquement le lecteur de pages complètes en conséquence (voir § C.4.2, point B.8).

D.9 **Prise en charge de la configuration sur serveur :** Il est recommandé de fournir une base de données d'authentification qui peut également être utilisée dans une configuration basée sur un serveur. Dans ce cas, différents logiciels d'authentification seraient en mesure d'accéder à une base de données d'authentification unique. En outre, deux bases de données d'authentification ou plus pourraient être exploitées sous forme de regroupement accessible à plusieurs logiciels d'authentification.

C.4.5 Fabricant de la base de données de référence

Bien que la base de données de référence ne fasse pas directement partie du système d'authentification (voir § C.2.1), elle peut être utilisée comme source d'information complémentaire si l'authenticité d'un document ne peut être établie clairement sur la base de l'authentification automatique. Dans ce cas, la base de données de référence est en mesure d'aider l'opérateur en lui fournissant des informations détaillées sur le modèle de document correspondant, par exemple des images de haute qualité des éléments, des explications textuelles et des informations sur les contrefaçons courantes (destinées à l'inspection de deuxième ligne/services auxiliaires). Un exemple de base de données de référence fournie par l'Union européenne est le système FADO (False and Authentic Documents Online). Le pendant du système FADO accessible au public est le PRADO[14] (Registre public en ligne de documents authentiques d'identité et de voyage).

14. https://www.consilium.europa.eu/prado/en/homeindex.html

En cas d'utilisation, certaines implications pratiques doivent être prises en compte par le fabricant de la base de données de référence. La présente section aborde ces implications sous forme de recommandations :

E.1 **Fournir une sortie automatique :** La base de données de référence doit recevoir et traiter un lien non ambigu vers un modèle de document en tant qu'entrée du processus d'identification. Il doit également fournir en sortie un ensemble de données de référence correspondant au lien.

E.2 **Permettre la sélection manuelle de l'ensemble de données :** Outre la sélection automatique d'un ensemble de données de référence, un opérateur doit également être en mesure de rechercher et de choisir manuellement un ensemble de données spécifique via une GUI.

E.3 **Fournir des informations détaillées sur les documents authentiques :** La base de données de référence contient des informations sur les documents authentiques et peut être accompagnée de descriptions liées de falsifications typiques. Les propriétés spécifiques des modèles de documents de référence doivent être décrites en détail et chaque contenu doit avoir une description textuelle.

Dans ce contexte, il convient de mentionner qu'une base de données telle que EDISON-TD peut également être prise en considération. Afin d'accroître l'utilisation des bases de données commerciales, les mécanismes décrits dans la recommandation D.1 peuvent être utilisés.

C.4.6 Responsable opérationnel

Le *responsable opérationnel* est l'organisation responsable de l'administration et de la gestion de tous les processus liés au fonctionnement de l'infrastructure d'authentification. Les opérateurs sont des membres du personnel du responsable opérationnel qui interagissent directement avec le système d'authentification.

La réalisation concrète de l'opération planifiée dépend du scénario d'inspection. Ci-dessous les exemples de scénarios :

- **Contrôle fixe aux frontières** (en abrégé SBC) : Dans ce cas, les autorités gouvernementales chargées du contrôle fixe aux frontières assument le rôle de responsable opérationnel (par exemple, la police des frontières). Habituellement, pour cette configuration, les opérateurs sont très familiers avec la vérification optique des documents. Le champ d'inspection est immense en raison du nombre élevé et de la diversité des documents contrôlés. En outre, le système nécessite une interaction et une évaluation poussées des opérateurs qui interagissent directement avec le système et le détenteur du document.

- **Contrôle automatisé des frontières par des portes ABC** (en abrégé ABC) : Dans ce scénario, les autorités gouvernementales des portes ABC assument également le rôle de responsable opérationnel, qui se concentre souvent davantage sur une authentification rapide des documents que sur une authentification approfondie. Dans ce cas, les opérateurs sont également des gardes-frontières bien formés et supervisent généralement un ensemble de portes ABC respectant une visualisation minimaliste. Contrairement au contrôle fixe aux frontières, le système est utilisé par les voyageurs et nécessite donc des orientations approfondies, qui sortent du cadre de ce manuel.

- **Authentification de documents à des fins commerciales** (en abrégé CP) : Dans ce cas, les entités commerciales assument le rôle de responsable opérationnel (par exemple, dans les banques). Contrairement aux scénarios mentionnés précédemment, les opérateurs ne sont généralement pas familiarisés avec la vérification optique des documents et la portée de l'inspection est généralement plus réduite que pour le contrôle aux frontières.

Les capacités des composants acquis doivent être en adéquation avec les besoins du responsable opérationnel et les exigences du scénario de déploiement. Dans cette section, les recommandations destinées aux fabricants de lecteurs de pages complètes (voir § C.4.2), de logiciels d'authentification (voir § C.4.3), de bases de données d'authentification (voir § C.4.4) et de bases de données de référence (voir § C.4.5) sont mises en correspondance avec les scénarios d'utilisation. Des recommandations pour le suivi en conformité avec les règles de protection des données sont présentées dans le § C.5.

Pour chaque scénario, le Tableau C-4 suivant résume l'utilisation raisonnable des recommandations pour le fabricant de lecteurs de pages complètes.

Tableau C-4. Recommandations pour les lecteurs de pages complètes classées par scénarios d'inspection

Fabricant de lecteurs de pages complètes				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
B.1	Assurer des longueurs d'onde appropriées du spectre lumineux	X	X	X
B.2	Assurer une résolution minimale	X	X	X
B.3	Fournir des formats d'image standard	X	X	X
B.4	Capture jusqu'à la taille ID-3	X	X	X
B.5	Assurer la capture de toutes les zones avec la même qualité	X	X	X
B.6	Assurer un temps de réponse court et une intensité constante	X	X	X
B.7	Assurer une qualité d'image constante	X	X	
B.8	Permettre le réglage de l'exposition à la lumière UV par le logiciel d'authentification	X	X	
B.9	Permettre la capture de plusieurs images UV	X		
B.10	Permettre des images sans reflets	X	X	
B.11	Fournir un mécanisme permettant de presser le document à plat sur la zone de capture	X	X	X
B.12	Permettre une utilisation d'une seule main	X	X	X
B.13	Fournir des orientations interactives aux utilisateurs		X	X[15]
B.14	Fournir du matériel avec un haut degré de robustesse	X	X	X

15. La compréhension des orientations pour les utilisateurs dépend fortement du cas d'utilisation commerciale.

Pour chaque scénario, le Tableau C-5 suivant résume l'utilisation raisonnable des recommandations pour le fabricant de produits logiciels d'authentification.

Tableau C-5. Recommandations pour les logiciels d'authentification classées par scénarios d'inspection

Fabricant de logiciels d'authentification				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
C.1	Permettre le traitement d'images préenregistrées16	X		
C.2	Permettre le traitement d'images provenant de différentes sources matérielles	X	X	X
C.3	Abstraire l'interface utilisateur graphique (GUI) du logiciel et du matériel d'authentification	X	X	X
Détection de documents				
C.4	Détection automatique et manuelle des documents	X	X[17]	
C.5	Compenser la rotation et recadrer la page de données capturées en conséquence	X	X	X
C.6	Détecter le document en fonction de la présence optique	X	X	X
Identification				
C.7	Identifier le modèle de document	X	X	X
C.8	Permettre une identification rapide au moyen de la ZLA	X	X	X
C.9	Fournir une solution de repli si la ZLA n'est pas lisible sous la lumière IR	X	X	X
C.10	Fournir un modèle de document sans ambiguïté	X		
C.11	Permettre une identification partielle	X		
C.12	Permettre l'identification manuelle	X		
C.13	Identifier les cartes d'identité sur les deux faces	X	X	X
C.14	Identifier les spécimens de documents	X	X	X

16. Cette recommandation est importante pour l'évaluation des produits logiciels d'authentification.
17. La détection manuelle des documents n'est pas applicable dans le scénario du contrôle automatisé aux frontières.

Fabricant de logiciels d'authentification				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
Vérification				
C.15	Effectuer un nombre minimum de contrôles spectralement sélectifs	X	X	X
C.16	Effectuer un contrôle de cohérence de la ZLA	X	X	X
C.17	Effectuer des contrôles dans toutes les catégories	X	X	X
C.18	Vérifier la présence de la puce	X	X	X
C.19	Vérifier les motifs dynamiques	X	X	X
C.20	Combiner les routines de contrôle si nécessaire	X	X	X
C.21	Effectuer des routines de contrôle redondantes sur plusieurs positions	X		X
C.22	Effectuer des routines de contrôle redondantes sur plusieurs couleurs UV	X		
C.23	Lier et vérifier les deux faces d'une carte d'identité	X	X	X
C.24	Permettre la vérification croisée des données personnelles sur plusieurs pages	X	X	X
C.25	Effectuer des routines de contrôle en fonction de l'importance	X	X	X
C.26	Prendre en considération l'écart des éléments	X	X	X
C.27	Détecter les attaques génériques	X	X	X
Visualisation				
C.28	Afficher tous les contrôles de documents dans une seule GUI	X	X	X
C.29	Toujours montrer la zone de résumé du processus	X	X	X
C.30	Afficher la zone optique générale sur la page d'accueil	X		
C.31	Sélectionnez plus de détails en un seul clic	X	X	
C.32	Afficher les résultats avec des feux de signalisation	X	X	X
C.33	Fournir une mise en correspondance des résultats conformément à BSI-TR-03135	X	X	X
C.34	Fournir une mise en correspondance des résultats minimaliste	X	X	X

Fabricant de logiciels d'authentification				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
C.35	Afficher les détails dans une zone optique détaillée	X		
C.36	Orienter les utilisateurs pendant la lecture des documents	X	X	X
C.37	Afficher des informations provenant de bases de données centrales	X		
C.38	Fournir une configuration homogène pour les DVLM	X		X
C.39	Orienter les opérateurs dans la vérification de plusieurs pages	X		
C.40	Permettre la comparaison du contenu du passeport et du visa/permis de séjour électronique	X		
C.41	Ne surligner que les irrégularités	X	X	X
C.42	Afficher les erreurs dans la zone de résumé du processus	X	X	X
C.43	Erreurs d'affichage dans la zone optique générale	X		
C.44	Afficher les erreurs dans la zone optique détaillée	X		
C.45	Affichage des erreurs de comparaison des passeports et des visas/permis de séjour électroniques	X		
Journalisation				
C.46	Journaux XML conformément à BSI-TR-03135	X	X	X
C.47	Permettre l'enregistrement de données d'image facultatives	X	X	X
C.48	Fournir des capacités d'anonymisation	X	X	X

Pour chaque scénario, le Tableau C-6 suivant résume l'utilisation raisonnable des recommandations pour le fabricant de bases de données d'authentification.

Tableau C-6. Recommandations pour les bases de données d'authentification classées par scénarios d'inspection

Fabricant de la base de données d'authentification				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
D.1	Échanger des informations sur les nouveaux modèles de documents ou les contrefaçons	X	X	
D.2	Mettre régulièrement à jour la base de données	X	X	X
D.3	Fournir des mises à jour progressives	X	X	X
D.4	Fournir une documentation suffisante sur les changements	X	X	X
D.5	Fournir un contenu réduit			X
D.6	Attribuer des contrôles avec des niveaux d'importance	X	X	X
D.7	Fournir différents modes de fonctionnement	X	X	X
D.8	Fournir des informations sur l'exposition aux UV propres au modèle de document	X	X	X
D.9	Prise en charge de la configuration sur serveur	X	X	X

Pour chaque scénario, le Tableau C-7 suivant résume l'utilisation raisonnable des recommandations pour le fabricant de bases de données de référence.

Tableau C-7. Recommandations pour les bases de données de référence classées par scénarios d'inspection

Fabricant de la base de données de référence				
N°	*Brève description*	*Scénario d'utilisation*		
		SBC	ABC	CP
E.1	Fournir une sortie automatique	X		
E.2	Permettre la sélection manuelle de l'ensemble de données	X		X[18]
E.3	Fournir des informations détaillées sur les documents authentiques	X		X[18]

C.5 SURVEILLANCE EN CONFORMITÉ AVEC LA PROTECTION DES DONNÉES

Un processus d'authentification optique peut aboutir à un résultat inattendu pour l'une des raisons suivantes :

- Une contrefaçon a été détectée.
- Une contrefaçon a été classée comme authentique.
- Un document authentique a été classé comme contrefait.
- Une erreur de manipulation du lecteur de pages complètes s'est produite, par exemple, le document a été retiré du lecteur pendant l'authentification.
- Le modèle de document n'a pas pu être identifié.

Dans ces cas, il est crucial pour le responsable opérationnel d'être capable d'analyser la raison de la mauvaise décision. Ainsi, les informations obtenues lors de la procédure d'authentification — y compris éventuellement des informations personnelles — doivent être enregistrées et analysées. Cela soulève directement des problèmes de protection des données, car il n'est pas permis de stocker des données personnelles, même cryptées, sans le consentement du détenteur du document ou une raison déterminée. Les recommandations suivantes peuvent être formulées pour le responsable opérationnel :

F.1 **Enregistrer les rapports d'authentification :** Les informations relatives à la procédure d'authentification sans données personnelles (par exemple, le modèle de document identifié, les résultats de l'authentification, les résultats de la routine de contrôle, etc.) doivent être enregistrées conformément à BSI-TR-03135. L'ensemble de données réelles, la ZLA et la ZIV sont par conséquent exclues de

18. Compte tenu de CP, il est important d'ajuster le niveau de connaissance, en fonction du cas d'utilisation.

l'enregistrement. Ces informations ne sont pas critiques du point de vue du temps et peuvent être utilisées pour des analyses statistiques.

F.2 **Mettre en place une boucle de rétroaction avec le fabricant :** Le retour d'information régulier de l'opération peut être utilisé pour optimiser le logiciel d'authentification. Par conséquent, les informations de rapport précisées dans F.1 devraient être transmises régulièrement au fabricant du logiciel d'authentification.

F.3 **Stocker l'ensemble de données réelles non modifiées si elles sont admissibles :** L'analyse des erreurs peut être effectuée au mieux sur le même ensemble de données réelles qui a été fourni pour l'authentification. Il est donc recommandé de stocker les ensembles de données réelles non modifiées dans le schéma XML défini par BSI-TR-03135, si cela peut être fait en tenant compte des préoccupations relatives à la confidentialité des données. Les possibilités d'enregistrement suivantes, y compris les images, existent :

a) *Stocker un ensemble de données réelles avec le consentement du détenteur du document :* Si le scénario le permet, l'ensemble de données réelles utilisées pour l'authentification peut être stocké, si le consentement du détenteur du document a été recueilli au préalable sous forme écrite. Cette façon de faire n'est concevable que pour des scénarios permettant une communication avec le détenteur du document, comme les pilotes, et non pour un fonctionnement permanent. En outre, les ensembles de données réelles doivent être effacés de manière irrémédiable après une période définie par contrat.

b) *Stocker l'ensemble de données réelles en cas d'erreur :* Les données à caractère personnel peuvent être conservées pendant une période définie par contrat, s'il existe une raison déterminée de les conserver, par exemple si une erreur s'est produite lors de l'authentification. Si le scénario le permet, cette période peut être utilisée pour l'analyse des erreurs sur l'ensemble de données réelles non modifiées, qui doit ensuite être supprimé de manière irrémédiable.

c) *Enregistrer les régions respectueuses de la vie privée :* Pour éviter les problèmes de confidentialité des données tout en préservant les possibilités d'analyse grossière, seules les images recadrées « respectueuses de la vie privée » affichant la zone de recherche des routines de contrôle peuvent être enregistrées. Ces régions d'intérêt ne doivent pas contenir la totalité de l'image faciale, la ZLA ou la ZIV et peuvent être stockées pour tous les processus d'authentification sans restriction de temps dans le schéma XML défini par BSI-TR-03135.

F.4 **Anonymiser les images si cela est possible :** Une autre proposition pour éviter les problèmes de confidentialité des données, tout en conservant l'ensemble complet de données réelles sans restriction de temps, consiste à anonymiser les données personnelles sur l'ensemble de données réelles. Grâce à cette méthode, les zones contenant des données personnelles sont difficiles à analyser, tandis que les parties du document non liées à des personnes restent entièrement analysables.

Note.— Pour clarifier les préoccupations relatives à la confidentialité des données : Les préoccupations relatives à la confidentialité des données mentionnées dans les recommandations F.1 à F.4 doivent être clarifiées par le responsable opérationnel, par exemple au moyen d'un concept de confidentialité des données. Les recommandations relatives au stockage de l'ensemble de données réelles formulées aux points F.3 et F.4 peuvent être combinées, par exemple en stockant des régions respectueuses de la vie privée.

C.6 BIBLIOGRAPHIE

[BSI-TR-03135] BSI, Authentification par machine pour les applications du secteur public, TR-03135, 2017. url https://www.bsi.bund.de/tr03135/

[FRONTEX-ABC] FRONTEX : *Best Practice Technical Guidelines for Automated Border Control (ABC)* [Lignes directrices techniques des meilleures pratiques pour le contrôle automatisé des frontières (ABC)] Systems, 2012

— — — — — — — —

APPENDICE D À LA PARTIE 2
(INFORMATIF)

PRÉVENTION DE LA FRAUDE LIÉE AU PROCESSUS DE DÉLIVRANCE

D.1 PORTÉE

Le présent appendice décrit les risques de fraude liés au processus de demande et de délivrance des DVLM. Ces risques sont une conséquence des avantages que confère la possession d'un DVLM qui peut servir à confirmer l'identité et la citoyenneté du titulaire. Cet appendice recommande des précautions que peut prendre un État émetteur pour empêcher les fraudes.

D.2 LA FRAUDE ET SA PRÉVENTION

La fraude perpétrée dans le cadre du processus de délivrance peut se classer dans les principaux types suivants :

- vol et remplissage de DVLM vierges authentiques pour leur donner l'apparence de documents valides ;
- demande de DVLM présentée sous une fausse identité, en utilisant des preuves authentiques de citoyenneté et/ou d'identité volées à une autre personne, ou obtenues indûment de quelque autre façon ;
- demande de DVLM présentée sous une fausse identité, en utilisant de fausses preuves fabriquées de citoyenneté et/ou d'identité ;
- utilisation de DVLM faussement déclarés perdus ou volés ou dont la perte ou le vol n'ont pas été déclarés pour les fournir à des personnes qui pourraient s'en servir pour une fraude basée sur la ressemblance ou avec des substitutions répétées de photographies ;
- recours à des agents en charge des DVLM pour manipuler le système afin de délivrer un DVLM en dérogeant aux règles.

Il existe deux autres catégories de fraude, dans lesquelles les demandeurs font une demande sous leur propre identité, mais avec l'intention de se rendre complice d'une utilisation frauduleuse ultérieure du DVLM, par :

- modification d'un document émis de façon légitime pour l'adapter à un détenteur autre que la personne à qui le DVLM a été délivré ;
- demande de DVLM avec l'intention de le donner ou de le vendre à une personne qui ressemble au titulaire légitime.

D.3 MESURES RECOMMANDÉES CONTRE LA FRAUDE

Pour combattre les menaces qui viennent d'être mentionnées, il est recommandé que l'autorité nationale de délivrance des DVLM prenne les mesures suivantes, compte tenu de la disponibilité de ressources suffisantes pour les mettre en œuvre.

Une personne dûment qualifiée devrait être nommée chef de la sécurité, relevant directement du directeur général de l'autorité de délivrance. Le chef de la sécurité devrait avoir la responsabilité de veiller à ce que des procédures de sécurité soient établies, observées et actualisées, selon les besoins.

Un responsable de la sécurité devrait être désigné à chaque lieu de délivrance de DVLM. Relevant directement du chef de la sécurité, le responsable de la sécurité devrait avoir la responsabilité de la mise en œuvre et de l'actualisation des procédures de sécurité.

Des procédures de contrôle de sécurité devraient être appliquées pour que le personnel ne soit recruté qu'après qu'une enquête aura permis de vérifier l'identité du candidat, de s'assurer qu'il n'a pas de casier judiciaire et de vérifier la solidité de sa situation financière. Des contrôles de suivi devraient aussi être effectués régulièrement pour déceler les personnes dont la situation a changé et qui pourraient être amenées par leurs nouvelles circonstances à succomber à la tentation de s'engager dans des activités frauduleuses.

Tout le personnel de l'autorité de délivrance des DVLM devrait être encouragé à adopter une attitude positive à l'égard des questions de sécurité. Un système devrait être mis en place pour récompenser tout agent qui rend compte d'incidents ou qui suggère des mesures visant à empêcher la fraude.

Des contrôles devraient être établis pour la comptabilisation de composants clés tels les livrets vierges et les films de sécurité. Chacun de ces articles devrait porter un numéro de série unique et être conservé sous clé dans un lieu d'entreposage sécurisé approprié. Seul le nombre nécessaire de ces articles devrait être sorti au début de chaque journée ou de chaque quart de travail. Les articles devraient être comptés et les chiffres vérifiés par deux membres du personnel, qui devraient aussi en enregistrer les numéros uniques. À la fin du quart, la personne à qui les articles ont été remis devrait en rendre compte en détail, sous la forme de documents personnalisés ou de produits défectueux. Tous les articles devraient être retournés à l'entrepôt sécurisé à la fin de la période de travail, encore une fois après comptage par deux personnes et enregistrement des numéros uniques. Les registres devraient être conservés pendant au moins la durée de vie des DVLM délivrés.

Les produits ou matériaux défectueux devraient être détruits dans des conditions contrôlées, après enregistrement de leurs numéros uniques.

Le processus de délivrance devrait être divisé en opérations distinctes, effectuées dans des locaux séparés à l'intérieur de l'établissement. L'objet est d'empêcher qu'une personne puisse accomplir l'ensemble du processus de délivrance sans se rendre dans une ou plusieurs zones auxquelles elle n'est pas autorisée à accéder.

D.4 PROCÉDURES POUR COMBATTRE LES DEMANDES FRAUDULEUSES

Les procédures suivantes sont recommandées pour empêcher la délivrance d'un DVLM authentique à la suite de la réception d'une demande frauduleuse.

Le service de délivrance des DVLM devrait nommer un nombre approprié de spécialistes de la lutte contre la fraude (SLF), ayant reçu une formation de haut niveau dans la détection de tous les types de fraude liés aux demandes de DVLM. Un de ces spécialistes au moins devrait être présent à tout endroit où des demandes de DVLM sont instruites et où sont reçus des demandeurs. Un SLF devrait toujours être disponible pour fournir un appui à ceux qui ont pour tâche d'instruire les demandes [agents d'autorisation (AA)] et apporter ainsi son concours au traitement réservé à toute demande suspecte. Les SLF devraient régulièrement dispenser des formations aux AA pour les sensibiliser davantage aux risques de fraude.

Les autorités de délivrance des DVLM devraient établir des liens étroits avec les autorités qui délivrent les « documents sources », tels les extraits d'actes de naissance, certificats de mariage et permis de conduire. L'accès à une base de

données de certificats de décès aide à la prévention de la fraude si une demande de DVLM est faite au nom d'une personne décédée. L'État devrait veiller à ce que les services qui conservent les actes de naissance, de mariage et de décès soient rapprochés pour s'assurer qu'ils concordent et à ce que les données soient mises en mémoire dans une base de données à laquelle le service de délivrance des DVLM devrait avoir un accès sécurisé. Le but est de faciliter une vérification rapide de l'authenticité des documents sources qui ont été présentés et de s'assurer, par exemple, qu'une demande n'est pas présentée au nom d'une personne décédée. Les personnes qui demandent un DVLM et qui n'en possédaient pas auparavant devraient être invitées à se présenter personnellement au service de délivrance des DVLM, munies des documents sources, pour une entrevue avec un AA et, s'il y a lieu, un SLF.

Une entrevue peut également être utilisée pour traiter les demandes de remplacement d'un DVLM qui vient à expiration. Une autre possibilité, pourvu que le service de délivrance des DVLM possède une base de données adéquate d'informations personnelles, incluant les portraits, est d'instruire les demandes de DVLM de remplacement sur la base de documents envoyés par la poste, y compris une nouvelle photo d'identité. En pareil cas, il est souhaitable que la demande et la nouvelle photo d'identité soient visées par un répondant. La restitution du DVLM venant à expiration devrait être exigée lors de la demande de nouveau document.

Le service de délivrance des DVLM devrait instaurer des procédures visant à empêcher la délivrance frauduleuse de plus d'un DVLM à une personne qui aurait tenté d'assumer plus d'une identité. Les vérifications par ordinateur dans la base de données des portraits stockés par les techniques de reconnaissance faciale et, le cas échéant, celle des empreintes digitales peuvent contribuer à ce processus.

Les procédures mises en place au service de délivrance des DVLM devraient empêcher qu'un demandeur choisisse l'agent d'autorisation avec lequel il souhaite traiter. Inversement, le flux des travaux devrait être tel qu'il empêche les agents de choisir les demandes qu'ils vont instruire.

La délivrance d'un DVLM à un jeune enfant devrait requérir la présence au service de délivrance, de préférence, de l'enfant et de ses deux parents. Cette recommandation vise à réduire les risques de trafic d'enfants et d'enlèvement d'enfants par un de leurs parents.

Le remplacement d'un DVLM déclaré perdu ou volé ne devrait être effectué qu'après des vérifications approfondies, incluant une entrevue personnelle avec le demandeur.

Il est recommandé que les détails sur les passeports perdus ou volés soient communiqués à la base de données d'INTERPOL, en particulier les numéros des documents. Cette base de données est accessible à tous les pays participants et peut servir à l'élaboration de listes de surveillance.

D.5 CONTRÔLE DES INSTALLATIONS DE DÉLIVRANCE

Un État devrait envisager de délivrer tous ses DVLM à partir d'un centre unique ou au maximum de deux centres, de manière à réduire le nombre de lieux d'entreposage de documents vierges et d'autres composants de sécurité. Il est possible d'assurer un contrôle bien plus rigoureux dans un centre de délivrance unique que dans plusieurs centres différents. Si la délivrance centralisée est adoptée, il faudra prévoir des centres où pourront avoir lieu, au besoin, les entrevues avec les demandeurs. De plus, étant donné que les DVLM normalisés ne peuvent pas être délivrés instantanément, un système devrait être mis en place pour la délivrance de DVLM d'urgence.

— — — — — — — —

APPENDICE E À LA PARTIE 2
(INFORMATIF)

CONSIDÉRATIONS ESSENTIELLES RELATIVES À L'ASF-SLTD

Prescriptions de la loi	Avant que les États ne puissent commencer à consigner des renseignements dans l'ASF-SLTD d'INTERPOL, ils doivent consulter leur législation pour déterminer s'ils ont l'autorité ou le mandat de donner un accès international à des éléments de renseignements des documents de voyage de leurs citoyens. S'il est nécessaire de modifier les lois, il est recommandé que les États prévoient des dispositions appropriées pour : 1. la collecte et le stockage des données ; 2. les dispositions relatives à la protection de la vie privée (notamment la sécurité) ; 3. l'autorisation de diffuser des données à la communauté internationale ; 4. le cycle de vie et la non-répudiation des données.
Éléments de données	Un ensemble de données standard axé sur les détails du document plutôt que sur le titulaire du document a été élaboré pour l'échange de renseignements sur les documents de voyage perdus, volés ou révoqués. Les États doivent remplir les champs de données requis lorsqu'ils versent les renseignements dans la base de données : 1. numéro d'identification du document de voyage* ; 2. type de document (passeport ou autre) ; 3. code OACI de l'État émetteur ; 4. statut du document (par exemple, document vierge volé) ; 5. pays où a été commis le vol (obligatoire seulement pour les documents de voyage vierges volés). * Dans le cas d'un document de voyage personnalisé, il s'agit du numéro figurant dans la ZLA ; dans le cas d'un livret vierge, il s'agit du numéro de série, si les numéros sont différents.
Collecte de renseignements	Les États doivent veiller à ce que les outils employés pour recueillir les renseignements sur les documents de voyage perdus ou volés (par exemple, entrevues par téléphone, formulaires en ligne) soient exhaustifs et permettent d'obtenir de manière sûre tous les renseignements requis pour remplir le rapport ASF-SLTD.

Communication rapide de données précises	La force de l'ASF-SLTD d'INTERPOL repose sur la communication rapide de renseignements précis. Les États doivent donc veiller à mettre en place les systèmes et les processus nécessaires pour échanger des renseignements le plus rapidement possible afin d'intercepter toute tentative d'utilisation de documents perdus, volés ou révoqués aux contrôles frontaliers. Les États devraient s'efforcer de communiquer ces renseignements quotidiennement. En général, l'autorité de délivrance devrait, dès qu'elle apprend que le document de voyage n'est plus en possession de son titulaire légitime ou qu'il a été révoqué, enregistrer officiellement les renseignements reçus dans sa base de données nationale (si elle tient une telle base) et dans l'ASF-SLTD. Les États devraient aussi continuellement veiller à ce que les données soient précises et fiables. L'autorité de délivrance doit prendre soin d'éviter les erreurs de saisie et de fournir toutes les données du document requises, car elle est responsable de la communication exacte des renseignements. Les erreurs dans la communication des données peuvent perturber les voyages et être coûteuses tant pour le voyageur que pour l'État émetteur. Les États doivent donc prendre les mesures nécessaires pour veiller à l'exactitude de l'enregistrement et de la déclaration de documents de voyage perdus, volés ou révoqués. Il est recommandé que les États mettent en place un service d'intervention fonctionnant 24 heures sur 24 pour répondre rapidement aux demandes de renseignements supplémentaires faites par INTERPOL au nom des États qui demandent ces renseignements.
Optimisation des bases de données nationales sur les documents de voyage perdus, volés ou révoqués	Les États qui possèdent une base de données nationale sur les documents de voyage perdus, volés ou révoqués devraient envisager d'utiliser des moyens automatiques de transmission des renseignements à INTERPOL de manière à optimiser leurs efforts.

— FIN —

ISBN 978-92-9265-492-4