►**B**

DÉCISION D'EXÉCUTION (UE) 2021/1073 DE LA COMMISSION

du 28 juin 2021

établissant les spécifications techniques et les règles relatives à la mise en œuvre du cadre de confiance pour le certificat COVID numérique de l'UE établi par le règlement (UE) 2021/953 du Parlement européen et du Conseil

(Texte présentant de l'intérêt pour l'EEE)

(JO L 230 du 30.6.2021, p. 32)

Modifiée par:

		Journal officiel		
		n°	page	date
►**M1**	Décision d'exécution (UE) 2021/2014 de la Commission du 17 Novembre 2021	L 410	180	18.11.2021
►**M2**	Décision d'exécution (UE) 2021/2301 de la Commission du 21 décembre 2021	L 458	536	22.12.2021
►**M3**	Décision d'exécution (UE) 2022/483 de la Commission du 21 mars 2022	L 98	84	25.3.2022
►**M4**	Décision d'exécution (UE) 2022/1516 de la Commission du 8 septembre 2022	L 235	61	12.9.2022

▼B

DÉCISION D'EXÉCUTION (UE) 2021/1073 DE LA COMMISSION

du 28 juin 2021

établissant les spécifications techniques et les règles relatives à la mise en œuvre du cadre de confiance pour le certificat COVID numérique de l'UE établi par le règlement (UE) 2021/953 du Parlement européen et du Conseil

(Texte présentant de l'intérêt pour l'EEE)

Article premier

Les spécifications techniques relatives au certificat COVID numérique de l'UE établissant la structure des données générique, les mécanismes d'encodage et le mécanisme d'encodage de transport dans un format optique lisible par machine figurent à l'annexe I.

Article 2

Les règles à suivre pour compléter les certificats visés à l'article 3, paragraphe 1, du règlement (UE) 2021/953 figurent à l'annexe II de la présente décision.

Article 3

Les exigences définissant la structure commune de l'identifiant unique du certificat figurent à l'annexe III.

▼M1

Article 4

Les règles de gouvernance applicables aux certificats de clé publique en ce qui concerne le service passerelle pour le certificat COVID numérique de l'UE prenant en charge les aspects d'interopérabilité du cadre de confiance figurent à l'annexe IV.

Article 5

L'annexe V de la présente décision définit une structure de données commune coordonnée pour les données à inclure dans les certificats prévus à l'article 3, paragraphe 1, du règlement (UE) 2021/953, en utilisant un schéma "JavaScript Object Notation" (JSON).

▼M3

Article 5 bis

Échange de listes de révocation de certificats

1. Le cadre de confiance pour le certificat COVID numérique de l'UE permet l'échange de listes de révocation de certificats via le service passerelle central pour le certificat COVID numérique de l'UE (le «service passerelle») conformément aux spécifications techniques figurant à l'annexe I.

2. Lorsque les États membres révoquent des certificats COVID numériques de l'UE, ils peuvent communiquer des listes de révocation de certificats au service passerelle.

▼M3

3. Lorsque les États membres communiquent des listes de révocation de certificats, les autorités de délivrance conservent une liste des certificats révoqués.

4. Lorsque des données à caractère personnel sont échangées via le service passerelle, le traitement est limité à la finalité consistant à soutenir l'échange d'informations relatives à la révocation. Ces données à caractère personnel ne sont utilisées qu'aux fins de vérifier le statut de révocation des certificats COVID numériques de l'UE délivrés dans le cadre du règlement (UE) 2021/953.

5. Les informations communiquées au service passerelle comprennent les données suivantes, conformément aux spécifications techniques figurant à l'annexe I:

a) les identifiants uniques pseudonymisés des certificats révoqués;

b) la date d'expiration de la liste de révocation de certificats qui a été communiquée.

6. Lorsqu'une autorité de délivrance révoque des certificats COVID numériques de l'UE qu'elle a délivrés en vertu du règlement (UE) 2021/953 ou du règlement (UE) 2021/954 et qu'elle a l'intention d'échanger les informations à ce sujet via le service passerelle, elle lui transmet les informations visées au paragraphe 5 sous la forme de listes de révocation de certificats, dans un format sécurisé, conformément aux spécifications techniques figurant à l'annexe I.

7. Les autorités de délivrance fournissent, dans la mesure du possible, une solution pour informer les titulaires des certificats révoqués de la révocation de leur certificat et du motif de cette mesure au moment où celle-ci est appliquée.

8. Le service passerelle rassemble les listes de révocation de certificats reçues. Il fournit des outils permettant de diffuser les listes aux États membres. Il supprime automatiquement les listes conformément aux dates d'expiration indiquées pour chaque liste communiquée par l'autorité concernée.

9. Les autorités nationales ou les organismes officiels désigné(e)s des États membres qui traitent des données à caractère personnel dans le service passerelle sont les responsables conjoints du traitement des données. Les responsabilités respectives des responsables conjoints du traitement sont réparties conformément à l'annexe VI.

10. La Commission est le sous-traitant des données à caractère personnel traitées dans le cadre du service passerelle. En sa qualité de sous-traitant pour le compte des États membres, la Commission veille à la sécurité de la transmission et de l'hébergement des données à caractère personnel au sein du service passerelle et respecte les obligations du sous-traitant énoncées à l'annexe VII.

11. L'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement des données à caractère personnel au sein du service passerelle est testée, analysée et évaluée régulièrement par la Commission et par les responsables conjoints du traitement.

▼M3

Article 5 ter

Communication de listes de révocation de certificats par des pays tiers

Les pays tiers délivrant des certificats COVID-19 pour lesquels la Commission a adopté un acte d'exécution en vertu de l'article 3, paragraphe 10, ou de l'article 8, paragraphe 2, du règlement (UE) 2021/953 peuvent communiquer des listes de certificats COVID-19 révoqués relevant de cet acte d'exécution, que la Commission traitera, pour le compte des responsables conjoints du traitement, dans le service passerelle visé à l'article 5 *bis*, conformément aux spécifications techniques énoncées à l'annexe I.

Article 5 quater

Gouvernance du traitement des données à caractère personnel dans le service passerelle central pour le certificat COVID numérique de l'UE

1. Le processus décisionnel des responsables conjoints du traitement est encadré par un groupe de travail établi au sein du comité visé à l'article 14 du règlement (UE) 2021/953.

2. Les autorités nationales ou les organismes officiels désigné(e)s des États membres qui traitent des données à caractère personnel dans le service passerelle en qualité de responsables conjoints du traitement désignent des représentants pour siéger au sein de ce groupe.

▼M1

Article 6

La présente décision entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

▼B

La présente décision entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

▼B

ANNEXE I

FORMAT ET GESTION DE LA CONFIANCE

Structure de données générique, mécanismes d'encodage et mécanisme d'encodage de transport dans un format optique lisible par machine (ci-après dénommé «QR»)

1. **Introduction**

Les spécifications techniques décrites dans la présente annexe contiennent une structure de données générique et des mécanismes d'encodage pour le certificat COVID numérique de l'UE (*EU Digital COVID Certificate* — DCC). Elles définissent également un mécanisme d'encodage de transport dans un format optique lisible par machine (*Quick Response* — QR), qui peut être affiché sur l'écran d'un appareil mobile ou être imprimé. Les formats du conteneur du certificat sanitaire électronique figurant dans les présentes spécifications sont génériques, mais, dans ce contexte, ils servent à porter le DCC.

2. **Terminologie**

Aux fins de la présente annexe, on entend par «émetteurs» les organismes qui utilisent les présentes spécifications pour délivrer des certificats sanitaires et par «vérificateurs» les organismes acceptant les certificats sanitaires comme preuve du statut sanitaire. On entend par «participants» les émetteurs et les vérificateurs. Certains aspects définis dans la présente annexe, tels que la gestion d'un espace de noms et la distribution des clés cryptographiques, doivent faire l'objet d'une coordination entre les participants. Il est supposé qu'une partie, ci-après dénommée le «secrétariat», accomplit ces tâches.

3. **Format du conteneur du certificat sanitaire électronique**

Le format du conteneur du certificat sanitaire électronique (*Electronic Health Certificate* — «HCERT») est conçu pour fournir un véhicule uniforme et normalisé pour les certificats sanitaires délivrés par les différents émetteurs (ci-après les «émetteurs»). Les présentes spécifications ont pour objet d'harmoniser la manière dont ces certificats sanitaires sont représentés, encodés et signés dans le but d'en faciliter l'interopérabilité.

La capacité de lire et d'interpréter un DCC délivré par un émetteur requiert une structure de données commune et un accord sur la signification de chaque champ de données de la charge utile. Pour faciliter cette interopérabilité, on définit une structure de données commune coordonnée en utilisant un schéma «JSON» qui constitue le cadre du DCC.

3.1. *Structure de la charge utile*

La charge utile est structurée et encodée au format CBOR (*Concise Binary Object Representation* — représentation concise d'objet binaire) avec une signature numérique au format COSE (*CBOR Object Signing and Encryption* — signature et chiffrement d'objet en représentation concise d'objet binaire). Cette structure est communément appelée «jeton CBOR pour la toile» (*CBOR Web Token* — CWT) et est définie dans la RFC 8392 ([1]). La charge utile, telle que définie dans les sections suivantes, est transportée dans une revendication hcert.

L'intégrité et l'authenticité de l'origine des données de la charge utile doivent être vérifiables par le vérificateur. Pour permettre ce mécanisme, l'émetteur doit signer le CWT au moyen d'un système de signature électronique asymétrique tel que défini dans la spécification COSE (RFC 8152 ([2])).

3.2. *Revendications CWT*

3.2.1. Vue d'ensemble de la structure CWT

En-tête protégé

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

▼B

— Algorithme de signature (alg, étiquette 1)

— Identifiant de clé (*Key Identifier* — ci-après «kid», étiquette 4)

Charge utile

— Émetteur (*Issuer* — ci-après «iss», clé de revendication 1, facultatif, ISO 3166-1 alpha-2 de l'émetteur)

— Délivré le (*Issued At* — ci-après «iat», clé de revendication 6)

— Délai d'expiration (exp, clé de revendication 4)

— Certificat sanitaire (hcert, clé de revendication -260)

— Certificat COVID numérique de l'UE v1 (eu_DCC_v1, clé de revendication 1)

Signature

3.2.2. Algorithme de signature

Le paramètre de l'algorithme de signature (alg) indique quel algorithme est utilisé pour créer la signature. Il doit respecter voire être plus strict que les lignes directrices actuelles du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS) résumées dans les paragraphes suivants.

Un algorithme primaire et un algorithme secondaire sont définis. L'algorithme secondaire ne devrait être utilisé que si l'algorithme primaire n'est pas acceptable dans le cadre des règles et réglementations imposées à l'émetteur.

Afin de garantir la sécurité du système, toutes les mises en œuvre doivent intégrer l'algorithme secondaire. C'est pourquoi tant l'algorithme primaire que l'algorithme secondaire doivent être mis en œuvre.

Les niveaux définis par le SOG-IS pour les algorithmes primaire et secondaire sont les suivants:

— Algorithme primaire: l'algorithme primaire est l'algorithme de signature numérique à courbe elliptique (*Elliptic Curve Digital Signature Algorithm* — ECDSA) tel que défini à la section 2.3 de la norme (ISO/IEC 14888–3:2006), utilisant les paramètres P–256 définis à l'appendice D (D.1.2.3) de la norme (FIPS PUB 186–4) en combinaison avec l'algorithme de hachage SHA–256 tel que défini dans la fonction 4 de la norme (ISO/IEC 10118–3:2004).

Cela correspond au paramètre ES256 de l'algorithme COSE.

— Algorithme secondaire: l'algorithme secondaire est le RSASSA-PSS tel que défini dans la (RFC 8230 ([1])) avec un modulus de 2048 bits en combinaison avec l'algorithme de hachage SHA–256 tel que défini dans la fonction 4 de la norme (ISO/IEC 10118–3:2004).

Cela correspond au paramètre de l'algorithme COSE: PS256.

3.2.3. Identifiant de clé

La revendication d'identifiant de clé (kid) indique le certificat de signataire de documents (DSC) contenant la clé publique qui doit être utilisé par le vérificateur pour vérifier l'exactitude de la signature numérique. La gouvernance des certificats de clé publique, y compris les exigences applicables aux DSC, est décrite à l'annexe IV.

([1]) rfc8230 (ietf.org).

▼B

La revendication d'identifiant de clé (kid) est utilisée par les vérificateurs pour sélectionner la bonne clé publique à partir d'une liste de clés appartenant à l'émetteur indiqué dans la revendication d'émetteur (iss). Plusieurs clés peuvent être utilisées parallèlement par un émetteur pour des raisons administratives et lors de la reconduction des clés. L'identifiant de clé n'est pas un champ critique pour la sécurité. Pour cette raison, il peut également être placé dans un en-tête non protégé si nécessaire. Les vérificateurs doivent accepter les deux options. Si les deux options sont présentes, c'est l'identifiant de clé dans l'en-tête protégé qu'il y a lieu d'utiliser.

En raison du raccourcissement de l'identifiant (pour des raisons de limitation de la taille), la probabilité est faible, mais pas nulle, que la liste globale des certificats de signataire de documents (*Document Signer Certificates* — DSC) acceptés par un vérificateur puisse contenir des DSC avec un double kid. C'est la raison pour laquelle le vérificateur doit vérifier tous les DSC présentant ce kid.

3.2.4. Émetteur

La revendication d'émetteur (iss) est une valeur de chaîne qui peut, à titre facultatif, contenir le code pays ISO 3166-1 alpha-2 de l'entité délivrant le certificat sanitaire. Cette revendication peut être utilisée par un vérificateur pour identifier la série de DSC à utiliser pour la vérification. La clé de revendication 1 est utilisée pour identifier cette revendication.

3.2.5. Délai d'expiration

La revendication de délai d'expiration (exp) doit contenir un horodatage au format date numérique (comme précisé dans la RFC 8392 ([1]), section 2) indiquant la période pendant laquelle cette signature particulière sur la charge utile doit être considérée comme valide, après quoi un vérificateur doit rejeter la charge utile considérée comme ayant expiré. L'objectif du paramètre d'expiration est d'imposer une limite à la durée de validité du certificat sanitaire. La clé de revendication 4 est utilisée pour identifier cette revendication.

Le délai d'expiration ne doit pas dépasser la période de validité du DSC.

3.2.6. Délivré le

La revendication «délivré le» (iat) doit contenir un horodatage au format date numérique (comme précisé dans la RFC 8392 ([2]), section 2) indiquant la date à laquelle le certificat sanitaire a été créé.

Le champ «délivré le» ne doit pas contenir une date antérieure à la période de validité du DSC.

Les vérificateurs peuvent appliquer des mesures supplémentaires dans le but de limiter la validité du certificat sanitaire en fonction de la date de délivrance. La clé de revendication 6 est utilisée pour identifier cette revendication.

3.2.7. Revendication de certificat sanitaire

La revendication de certificat sanitaire (hcert) est un objet JSON (RFC 7159 ([3])) contenant les informations relatives au statut sanitaire. Plusieurs types de certificat sanitaire peuvent exister sous la même revendication, le DCC en étant un.

Le format JSON sert uniquement pour les schémas. Le format de représentation est le CBOR, tel que défini dans la (RFC 7049 ([4])). Il se peut que les développeurs des applications ne décodent ou n'encodent jamais vers et depuis le format JSON et qu'ils utilisent la structure en mémoire.

([1]) rfc8392 (ietf.org).
([2]) rfc8392 (ietf.org).
([3]) rfc7159 (ietf.org).
([4]) rfc7049 (ietf.org).

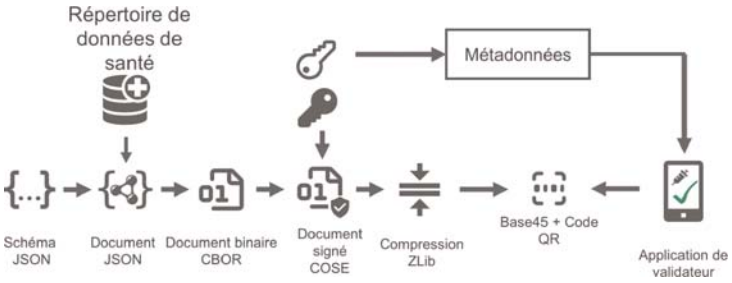
▼B

La clé de revendication à utiliser pour identifier cette revendication est -260.

Les chaînes de l'objet JSON doivent être normalisées conformément à la composition canonique des formes de normalisation (*Normalisation Form Canonical Composition* — NFC) définie dans la norme Unicode. Les applications de décodage devraient toutefois être permissives et robustes à ces égards, et l'acceptation de tout type de conversion raisonnable est fortement encouragée. Si des données non normalisées sont trouvées au cours du décodage ou dans le cadre de fonctions de comparaisons ultérieures, les mises en œuvre devraient se comporter comme si les données entrées étaient normalisées conformément à la NFC.

4. **Sérialisation et création de la charge utile du DCC**

En ce qui concerne la structure de sérialisation, la séquence suivante est utilisée:



Le processus commence par l'extraction de données, par exemple à partir d'un répertoire de données de santé (ou d'une source externe de données), structurant les données extraites conformément aux schémas de DCC définis. Lors de ce processus, la conversion au format de données défini et la transformation pour la lisibilité humaine peuvent avoir lieu avant le début de la sérialisation vers le format CBOR. Les abréviations (acronymes) des revendications doivent correspondre, dans tous les cas, aux noms d'affichage avant la sérialisation et après la désérialisation.

Le contenu des données nationales facultatives n'est pas autorisé dans les certificats délivrés conformément au règlement (UE) 2021/953 ([1]). Le contenu des données est limité aux éléments de données définis dans l'ensemble minimal de données spécifié dans le règlement (UE) 2021/953.

5. **Encodages de transport**

5.1. *Brut*

Pour les interfaces de données arbitraires, le conteneur du HCERT et ses charges utiles peuvent être transférés tels quels, en utilisant n'importe quel transport de données sous-jacent, sûr et fiable à 8 bits. Ces interfaces peuvent comprendre une communication en champ proche (*Near-Field Communication* — NFC), un Bluetooth ou un transfert via un protocole de couche application, par exemple le transfert d'un HCERT de l'émetteur vers l'appareil mobile du titulaire.

Si le transfert du HCERT de l'émetteur vers le titulaire est basé sur une interface de présentation uniquement (par exemple, SMS, courrier électronique), l'encodage de transport brut n'est évidemment pas applicable.

([1]) Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19, JO L 211 du 15.6.20211, p. 1.

▼B

5.2. *Code-barres*

5.2.1. Compression de la charge utile (CWT)

Afin de réduire la taille et d'améliorer la vitesse et la fiabilité du processus de lecture du HCERT, le CWT doit être comprimé, en utilisant le ZLIB (RFC 1950 ([1])) et le mécanisme de compression Deflate, au format défini dans la RFC 1951 ([2]).

5.2.2. Code-barres QR 2D

Afin de mieux gérer les équipements anciens conçus pour fonctionner sur des charges utiles ASCII, le CWT comprimé est encodé au format ASCII à l'aide de Base45 avant d'être encodé en un code-barres 2D.

Le format QR tel que défini dans la norme (ISO/IEC 18004:2015) doit être utilisé pour la génération du code-barres 2D. Un taux de correction d'erreur de «Q» (environ 25 %) est recommandé. Étant donné que Base45 est utilisé, le code QR doit utiliser l'encodage alphanumérique (mode 2, indiqué par les symboles 0010).

Afin que les vérificateurs puissent détecter le type de données encodées et sélectionner le système de décodage et de traitement approprié, les données encodées avec Base45 (conformément à la présente spécification) doivent avoir pour préfixe la chaîne d'identifiant de contexte «HC1:». Les versions futures de la présente spécification ayant une incidence sur la compatibilité rétrospective devront définir un nouvel identifiant de contexte, tandis que le caractère suivant la mention «HC» devra être tiré du jeu de caractères [1-9A-Z]. L'ordre des augmentations est défini selon cette séquence, c'est-à-dire d'abord [1-9], puis [A-Z].

Il est recommandé de faire apparaître le code optique sur le média de présentation avec une diagonale comprise entre 35 mm et 60 mm, afin de prendre en compte les lecteurs à optique fixe pour lesquels le média de présentation doit être placé à la surface du lecteur.

Si le code optique est imprimé sur papier à l'aide d'une imprimante à basse résolution (< 300 dpi), il faut veiller à ce que la forme carrée de chaque symbole (point) du code QR soit parfaitement respectée. Si l'échelle n'est pas proportionnelle, certaines lignes ou colonnes du QR comporteront des symboles rectangulaires, ce qui nuira à la lisibilité dans de nombreux cas.

6. **Format des listes de confiance (*trust lists*) (listes de CSCA et de DSC)**

Chaque État membre est tenu de fournir une liste mentionnant une ou plusieurs autorités nationales de signature de certificats (*Country Signing Certificate Authorities* — CSCA) et une liste de tous les certificats de signataire de documents (*Document Signer Certificates* — DSC) valides, et de tenir ces listes à jour.

6.1. *Simplification relative aux CSCA/DSC*

À partir de la présente version des spécifications, les États membres ne peuvent présumer que les informations relatives aux listes de révocation de certificat (*Certificate Revocation List* — CRL) puissent être utilisées, ou que la période d'utilisation des clés privées puisse être vérifiée par les responsables de la mise en œuvre.

Le principal mécanisme de validation consistera plutôt dans le fait que le certificat figure dans la version la plus récente de cette liste de certificats.

([1]) rfc1950 (ietf.org).
([2]) rfc1951 (ietf.org).

▼B

6.2. *Infrastructure à clé publique (ICP) des DVLMe (OACI) et centres de confiance*

Les États membres peuvent avoir recours à une CSCA distincte, mais peuvent également communiquer leurs certificats CSCA de DVLMe et/ou DSC existants; ils peuvent même choisir de se procurer ceux-ci auprès de centres de confiance (commerciaux) et les communiquer. Toutefois, un DSC doit toujours être signé par la CSCA communiquée par cet État membre.

7. **Considérations de sécurité**

Lors de la conception d'un système fondé sur la présente spécification, les États membres identifient, analysent et contrôlent certains éléments liés à la sécurité.

Les éléments qui devraient être pris en considération sont au minimum les suivants:

7.1. *Durée de validité de la signature du HCERT*

L'émetteur du HCERT est tenu de limiter la durée de validité de la signature en précisant le délai d'expiration de la signature. Le titulaire d'un certificat sanitaire est ainsi tenu de le renouveler périodiquement.

La durée de validité acceptable peut être déterminée par des contraintes pratiques. Par exemple, un voyageur peut ne pas avoir la possibilité de renouveler le certificat sanitaire au cours d'un voyage à l'étranger. Toutefois, il se peut également qu'un émetteur envisage la possibilité d'une quelconque compromission de la sécurité l'obligeant à retirer un DSC (ce qui invalide tous les certificats sanitaires délivrés au moyen de la clé dont la validité se situe encore dans leur période de validité). Les conséquences d'un tel événement peuvent être limitées en procédant régulièrement à la reconduction des clés de l'émetteur et en exigeant le renouvellement de tous les certificats sanitaires, à intervalles raisonnables.

7.2. *Gestion des clés*

La présente spécification repose largement sur des mécanismes cryptographiques solides pour garantir l'intégrité des données et l'authentification de l'origine des données. Il est donc nécessaire de préserver la confidentialité des clés privées.

La confidentialité des clés cryptographiques peut être compromise de différentes manières, par exemple:

— le processus de génération des clés peut être déficient, donnant lieu à des clés fragiles,

— les clés peuvent être vulnérables du fait d'une erreur humaine,

— les clés peuvent être volées par des délinquants externes ou internes,

— les clés peuvent être calculées à l'aide d'une analyse cryptographique.

Afin d'atténuer les risques liés à une éventuelle faiblesse de l'algorithme de signature, exposant les clés privées à une compromission par analyse cryptographique, la présente spécification recommande à tous les participants de mettre en œuvre un algorithme de signature secondaire de secours, fondé sur des paramètres différents ou un problème mathématique différent de celui du primaire.

En ce qui concerne les risques mentionnés liés aux modalités de fonctionnement des émetteurs, des mesures d'atténuation visant à garantir un contrôle efficace doivent être mises en œuvre, de manière à générer, stocker et utiliser les clés privées dans des modules matériels de sécurité (*Hardware Security Modules* — HSM). Il est vivement recommandé d'utiliser des HSM pour la signature des certificats sanitaires.

▼B

Indépendamment de la question de savoir si un émetteur décide d'utiliser ou non des HSM, il convient d'établir un calendrier de reconduction de clés dans lequel la fréquence des reconductions est proportionnelle à la vulnérabilité des clés aux réseaux externes, aux autres systèmes et au personnel. Un calendrier de reconduction bien choisi limite également les risques associés aux certificats sanitaires délivrés par erreur, car il permet à un émetteur de révoquer ces certificats par lots, en procédant au retrait d'une clé, si nécessaire.

7.3. *Validation des données d'entrée*

Les présentes spécifications peuvent être utilisées d'une manière qui implique de recevoir des données provenant de sources non fiables versées dans des systèmes qui peuvent être essentiels à la mission concernée. Afin de minimiser les risques associés à ce vecteur d'attaque, tous les champs d'entrée doivent être correctement validés par type, longueur et contenu des données. La signature de l'émetteur doit également être vérifiée avant tout traitement du contenu du HCERT. Toutefois, la validation de la signature de l'émetteur implique de parcourir d'abord l'en-tête protégé de l'émetteur, dans lequel un assaillant potentiel peut tenter d'injecter des informations soigneusement conçues pour compromettre la sécurité du système.

8. **Gestion de la confiance**

La signature du HCERT nécessite une clé publique à vérifier. Les États membres doivent mettre ces clés publiques à disposition. En fin de compte, chaque vérificateur doit disposer d'une liste de toutes les clés publiques auxquelles il est disposé à accorder sa confiance (étant donné que la clé publique ne fait pas partie du HCERT).

Le système se compose de (seulement) deux couches; pour chaque État membre, un ou plusieurs certificats au niveau du pays, qui signent chacun un ou plusieurs certificats de signataire de documents qui sont utilisés dans les opérations quotidiennes.

Les certificats des États membres sont appelés certificats des autorités nationales de signature de certificats (CSCA) et sont (généralement) des certificats autosignés. Les États membres peuvent en avoir plusieurs (par exemple, en cas de décentralisation régionale). Ces certificats CSCA signent régulièrement les certificats de signataire de documents (DSC) utilisés pour signer les HCERT.

Le «secrétariat» joue un rôle fonctionnel. Il doit agréger et publier régulièrement les DSC des États membres, après les avoir vérifiés par rapport à la liste des certificats CSCA (qui ont été transmis et vérifiés par d'autres moyens).

La liste des certificats DSC qui en résulte doit ensuite fournir l'ensemble agrégé de clés publiques acceptables (et les *kids* correspondants) que les vérificateurs peuvent utiliser pour valider les signatures sur les HCERT. Les vérificateurs sont tenus d'aller chercher et de mettre à jour régulièrement cette liste.

Ces listes par État membre peuvent être adaptées au format convenant à la situation nationale. Ainsi, le format de fichier de cette liste de confiance (*trust list*) peut varier; par exemple, il peut s'agir d'un JWKS signé (format JWK conformément à la RFC 7517 ([1]), section 5) ou de tout autre format spécifique à la technologie utilisée dans cet État membre.

Pour garantir la simplicité du processus, les États membres peuvent à la fois communiquer leurs certificats CSCA existants à partir de leurs systèmes de DVLMe conformes aux normes de l'OACI ou, comme l'OMS le recommande, créer un système spécifiquement pour ce domaine de la santé.

([1]) rfc7517 (ietf.org).

▼B

8.1. *Identifiant de clé (kids)*

L'identifiant de clé (*kid*) est calculé lors de l'établissement de la liste des clés publiques de confiance à partir des DSC et consiste en une empreinte SHA-256 tronquée (8 premiers octets) du DSC encodée au format DER (brut).

Les vérificateurs n'ont pas besoin de calculer le *kid* sur la base du DSC et peuvent directement mettre l'identifiant de clé figurant dans le certificat sanitaire délivré en correspondance avec le *kid* figurant sur la *trust list*.

8.2. *Différences par rapport au modèle de confiance de l'ICP des DVLMe (OACI)*

Bien que fondé sur les meilleures pratiques du modèle de confiance de l'ICP des DVLMe de l'OACI, il convient de simplifier quelque peu le modèle dans un souci de rapidité:

— l'État membre peut soumettre plusieurs certificats CSCA,

— la période de validité du DSC (utilisation de la clé) peut être fixée à n'importe quelle durée ne dépassant pas celle du certificat CSCA et peut être absente,

— le DSC peut contenir des identifiants de politique (utilisation étendue de la clé) qui sont propres aux certificats sanitaires,

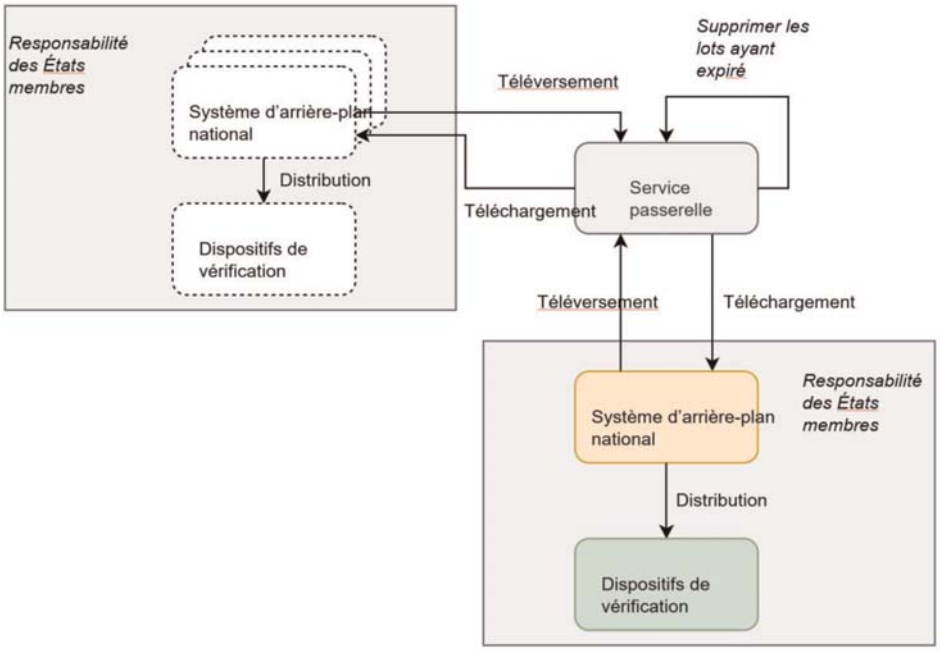
— les États membres peuvent choisir de ne jamais procéder à une vérification des révocations publiées et de se baser simplement sur les listes de DSC qu'ils obtiennent quotidiennement du secrétariat ou compilent eux-mêmes.

▼M3

9. **Solution de révocation**

9.1. *Établissement des listes de révocation de DCC (DCC Revocation List — DRL)*

Le service passerelle fournit des points de terminaison (*endpoints*) et une fonctionnalité pour conserver et gérer les listes de révocation:



▼**M3**

9.2. *Modèle de confiance*

Toutes les connexions sont établies par le modèle de confiance type du DCCG par les certificats NB_{TLS} et NB_{UP} (voir gouvernance des certificats). Toutes les informations sont assemblées en paquet et chargées par messages CMS afin que leur intégrité soit garantie.

9.3. *Construction des lots*

9.3.1. Lot (Batch)

Chaque liste de révocation contient une ou plusieurs entrées et est assemblée en paquet par lots contenant un ensemble de hachages (*hashes*) et leurs métadonnées. Un lot est immuable (*immutable*) et définit une date d'expiration qui indique à quel moment le lot peut être supprimé. La date d'expiration de tous les éléments du lot doit être exactement la même, ce qui signifie que les lots doivent être regroupés par date d'expiration et par DSC signataire. Chaque lot contient au maximum 1 000 entrées. Si la liste de révocation comporte plus de 1 000 entrées, des lots multiples sont créés. Une entrée ne peut apparaître que dans un seul lot au maximum. Le lot est empaqueté dans une structure CMS et signé par le certificat NB_{UP} du pays de chargement.

9.3.2. Index des lots (Batch Index)

Lorsqu'un lot (*batch*) est créé, il se voit attribuer un ID unique par le service passerelle et est automatiquement ajouté dans l'index. L'index des lots indique les dates modifiées, par ordre chronologique ascendant.

9.3.3. Comportement du service passerelle

Le service passerelle traite les lots de révocation sans aucune modification: il ne peut ni mettre à jour, ni supprimer les lots, ni y ajouter aucune information. Les lots sont transmis à tous les pays autorisés (voir chapitre 9.6).

Le service passerelle surveille activement les dates d'expiration des lots et supprime les lots ayant expiré. Une fois le lot supprimé, le service passerelle renvoie une réponse «HTTP 410 Gone» pour l'URL du lot supprimé. De ce fait, le lot apparaît dans l'index des lots comme étant «supprimé».

9.4. *Types de hachage (Hash Types)*

La liste de révocation contient des hachages qui peuvent représenter différents attributs/types de révocation. Ces types ou attributs sont indiqués lors de l'établissement des listes de révocation. Les types actuels sont les suivants:

Type	Attribut	Calcul du hachage
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Seuls les 128 bits initiaux des hachages encodés en chaînes base64 (*base64 strings*) sont placés dans les lots et utilisés pour identifier le DCC révoqué ([1]).

([1]) Veuillez également consulter, le point 9.5.1.2 pour les descriptions détaillées de l'API

▼**M3**

9.4.1. Type de hachage: SHA256 (Signature DCC)

Dans ce cas, le hachage est calculé sur les octets (*bytes*) de la signature COSE_SIGN1 venant du CWT. Pour les signatures RSA, la signature entière sera utilisée comme entrée. Pour les certificats signés EC-DSA, la formule utilise la valeur r comme entrée:

SHA256(r)

[nécessaire pour toutes les nouvelles mises en œuvre]

9.4.2. Type de hachage: SHA256(UCI)

Dans ce cas, le hachage est calculé sur la chaîne UCI (*UCI string*) encodée en UTF-8 et convertie en un *byte array*.

[déconseillé ([1]), mais supporté pour des raisons de rétrocompatibilité]

9.4.3. Type de hachage: SHA256(Issuing Country-Code+UCI)

Dans ce cas, CountryCode encodé en une chaîne UTF-8 (*UTF-8 string*) concaténé avec l'UCI encodé avec une chaîne UTF-8. Il est ensuite converti en un *byte array* et utilisé comme entrée pour la fonction de hachage.

[déconseillé[2], mais supporté pour des raisons de rétrocompatibilité]

9.5. *Structure de l'API*

9.5.1. API fournissant les entrées de révocation

9.5.1.1. Objectif

L'API fournit les entrées des listes de révocation par lots et comporte un index des lots.

9.5.1.2. Points de terminaison (*endpoints*)

9.5.1.2.1. Point de terminaison pour le téléchargement des listes de lots

Les points de terminaison suivent une conception simple et renvoient une liste de lots avec un petit *wrapper* fournissant des métadonnées (*metadata*). Les lots sont triés par *date*, par *ordre (chronologique) ascendant*:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    "more":true|false,
    "batches":
            [{
                "batchId": "{uuid}",
                "country": "XY",
                "date": "2021-11-01T00:00:00Z"
                "deleted": true | false
            }, ..
            ]
}
```

([1]) Cela signifie que cette fonctionnalité ne doit pas être envisagée pour de nouvelles mises en œuvre, mais doit être supportée pour les mises en œuvre existantes pendant une période bien définie.

▼M3

Remarque: Le résultat est limité par défaut à 1 000. Si le drapeau «more» est paramétré sur «true», la réponse indique qu'il est possible de télécharger davantage de lots. Pour télécharger davantage d'éléments, le client doit régler l'en-tête (*header*) If-Modified-Since sur une date qui ne doit pas être antérieure à la dernière entrée reçue.

La réponse contient un *JSON array* dont la structure est la suivante:

Champ	Définition
more	Drapeau booléen qui indique qu'il y a davantage de lots.
batches	*Array* avec les lots existants.
batchId	https://fr.wikipedia.org/wiki/Universally_unique_identifier
country	Code pays ISO 3166
date	ISO 8601 Date UTC. Date à laquelle le lot a été ajouté ou supprimé.
deleted	boolean. «True» si supprimé. Lorsque le drapeau «supprimé» est sélectionné, l'entrée peut être finalement retirée des résultats de la requête après 7 jours.

9.5.1.2.1.1. *Codes* de réponse

Code	Description
200	Tout OK.
204	Pas de contenu, si l'en-tête (*header*) «If-Modified-Since» n'a pas de correspondance.

En-tête de requête (Request Header)

En-tête	Obligatoire	Description
If-Modified-Since	Oui	Cet en-tête contient la dernière date téléchargée afin de n'obtenir que les résultats les plus récents. Lors de l'appel initial, l'en-tête devrait être réglé sur "2021-06-01T00:00:00Z".

9.5.1.2.2. Point de terminaison pour le téléchargement des lots

Les lots contiennent une liste d'identifiants de certificats:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

"country": "XY",

"expires": "2022-11-01T00:00:00Z",

▼**M3**

“kid”:“23S+33f=”,

“hashType”:“SIGNATURE”,

“entries”:[{

“hash”:“e2e2e2e2e2e2e2e2”

}, ..]

}

La réponse contient un CMS comportant une signature qui doit correspondre au certificat NB_{UP} du pays. Tous les éléments du *JSON array* contiennent la structure suivante:

Champ	Obligatoire	Type	Définition
expires	Oui	String	Date à laquelle l’élément peut être retiré. ISO8601 Date/heure UTC
country	Oui	String	Code pays ISO 3166
hashType	Oui	String	Type de hachage des entrées fournies (voir Types de hachage)
entries	Oui	JSON Object Array	Voir tableau Entrées
kid	Oui	String	KID encodé en base64 du DSC utilisé pour signer le DCC. Si le KID n’est pas connu, la chaîne 'UNKNOWN_KID' (à l’exclusion des ') peut être utilisée.

Remarques:

— Les lots sont regroupés par date d’expiration et par DSC — tous les éléments expirent en même temps et ont été signés par la même clé.

— L’heure d’expiration est une date/heure en UTC parce que l’EUDCC est un système mondial et que nous devons utiliser une heure dépourvue d’ambiguïté.

— La date d’expiration d’un DCC définitivement révoqué est fixée à la date d’expiration du DSC correspondant utilisé pour signer le DCC ou à l’heure d’expiration du DCC révoqué (auquel cas les heures *NumericDate/epoch* utilisées sont considérées comme se trouvant dans le fuseau horaire UTC).

— Le système d’arrière-plan national (*National Backend — NB:*) supprime des éléments de leur liste de révocation lorsque la date d’**expiration** est atteinte.

— Le *NB:* peut retirer des éléments de leur liste de révocation si le **kid** utilisé pour signer le DCC est révoqué.

▼**M3**

9.5.1.2.2.1. Entrées

Champ	Obligatoire	Type	Définition
hash	Oui	String	128 bits initiaux du hachage SHA256 encodés en une chaîne base64 (*base64 string*)

Remarque: L'objet des entrées ne contient actuellement qu'un hachage, mais c'est un objet qui a été choisi, plutôt qu'un *JSON array*, pour permettre la compatibilité avec les modifications à venir.

9.5.1.2.2.2. Codes de réponse

Code	Description
200	Tout OK.
410	*Batch gone.* Le lot peut être supprimé dans le système d'arrière-plan national.

9.5.1.2.2.3. En-têtes de réponse

En-tête	Description
ETag	ID du lot

9.5.1.2.3. Point de terminaison pour le chargement des lots

Le chargement est effectué sur le même point de terminaison au moyen du verbe (*Verb*) POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

```
{
    "country": "XY",
    "expires": "2022-11-01T00:00:00Z",
    "kid":"23S+33f=",
    "hashType":"SIGNATURE",
    "entries":[{
            "hash":"e2e2e2e2e2e2e2e2"
            }, ..]
}
```

Le lot est signé en utilisant le certificat NB_{UP}. Le service passerelle vérifie que la signature a été réglée par le NB_{UP} pour le *pays* concerné. Si la vérification de la signature échoue, le chargement échoue.

REMARQUE: Chaque lot est immuable (*immutable*) et ne peut pas être modifié après le chargement. Il peut toutefois être supprimé. L'ID de chaque lot supprimé est stocké, et tout chargement d'un nouveau lot portant le même ID est rejeté.

▼**M3**

9.5.1.2.4. Point de terminaison pour la suppression des lots

Un lot peut être supprimé sur le même point de terminaison au moyen du verbe (*Verb*) DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

“batchId”: “...”

}

ou, pour des raisons de compatibilité, au point de terminaison suivant au moyen du verbe (*Verb*) POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

“batchId”: “...”

}

9.6. *Protection de l’API/RGPD*

La présente section précise les mesures garantissant que la mise en œuvre respecte les dispositions du règlement (UE) 2021/953 en ce qui concerne le traitement des données à caractère personnel.

9.6.1. Authentification existante

Le service passerelle utilise actuellement le certificat NB_{TLS} pour authentifier les pays qui s’y connectent. Cette authentification peut être utilisée pour déterminer l’identité du pays connecté au service passerelle. Cette identité peut ensuite être utilisée pour mettre en œuvre le contrôle d’accès.

9.6.2. Contrôle d’accès

Pour pouvoir traiter légalement des données à caractère personnel, le service passerelle met en œuvre un mécanisme de contrôle de l’accès.

Le système passerelle met en œuvre une liste de contrôle d’accès (*Access Control List*) combinée à une sécurité fondée sur les rôles (*Role Based Security*). Ce système implique de tenir deux tableaux, l’un indiquant quels rôles peuvent appliquer quelles opérations à quelles ressources, l’autre indiquant quels rôles sont attribués à quels utilisateurs.

La mise en œuvre des contrôles requis par le présent document nécessite les trois rôles suivants:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Les points de terminaison (*endpoints*) suivants vérifient si l'utilisateur (*User*) dispose du rôle (*Role*) de RevocationListReader; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Les points de terminaison suivants vérifient si l'utilisateur dispose du rôle de RevocationUploader; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

POST/revocation-list

Les points de terminaison suivants vérifient si l'utilisateur dispose du rôle de RevocationDeleter; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Le service passerelle fournit également une méthode fiable permettant aux administrateurs de gérer les rôles liés aux utilisateurs de manière à réduire les risques d'erreurs humaines sans pour autant occasionner de charge pour les administrateurs fonctionnels.

▼M1

ANNEXE II

RÈGLES POUR COMPLÉTER LE CERTIFICAT COVID NUMÉRIQUE DE L'UE

Les règles générales concernant les ensembles de valeurs établies dans la présente annexe visent à assurer l'interopérabilité au niveau sémantique et permettent des mises en œuvre techniques uniformes pour le certificat COVID numérique de l'UE. Les éléments figurant dans la présente annexe peuvent être utilisés pour les trois contextes différents (vaccination/test/rétablissement), tels que prévus par le règlement (UE) 2021/953. Seuls les éléments nécessitant une normalisation sémantique au moyen d'ensembles de valeurs codées sont énumérés dans la présente annexe.

La traduction des éléments codés dans la langue nationale relève de la responsabilité des États membres.

Pour tous les champs de données non mentionnés dans les descriptions des ensembles de valeurs ci-dessous, l'encodage est décrit à l'annexe V.

Si, pour une raison quelconque, les systèmes de codes privilégiés énumérés ci-dessous ne peuvent pas être utilisés, il est possible d'avoir recours à d'autres systèmes de codes internationaux et il y a lieu d'établir des orientations sur la manière de faire correspondre les codes de l'autre système à ceux du système de codes privilégié. Le texte (les noms d'affichage) peut être utilisé, dans des cas exceptionnels, comme mécanisme de sauvegarde lorsqu'aucun code approprié n'est disponible dans les ensembles de valeurs définis.

Les États membres qui utilisent d'autres codages dans leurs systèmes mettent ces codes en correspondance avec les ensembles de valeurs décrits. Les États membres sont responsables de ces éventuelles mises en correspondance.

►M4 Étant donné que certains ensembles de valeurs fondés sur les systèmes de codage prévus dans la présente annexe, tels que ceux utilisés pour le codage des vaccins et des tests de détection d'antigènes, sont souvent modifiés, ils sont publiés et régulièrement mis à jour par la Commission avec le soutien du réseau «Santé en ligne» et du comité de sécurité sanitaire (CSS). ◄ Les ensembles de valeurs mis à jour sont publiés sur le site web concerné de la Commission, ainsi que sur la page web du réseau "Santé en ligne". Un historique des changements est fourni.

1. **Maladie ou agent ciblés/Maladie ou agent dont le titulaire s'est rétabli: COVID-19 (SARS-CoV-2 ou un de ses variants)**

   À utiliser dans les certificats 1, 2 et 3.

   Le code suivant est utilisé:

Code	Affichage	Nom du système de codes	URL du système de codes	OID du système de codes	Version du système de codes
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **Vaccin ou prophylaxie contre la COVID-19**

   Système de codes privilégié: SNOMED CT ou classification ATC.

   À utiliser dans le certificat 1.

   Des exemples de codes à utiliser issus des systèmes de codes privilégiés sont les codes SNOMED CT 1119305005 (vaccin antigénique SARS-CoV-2), 1119349007 (vaccin à ARNm SARS-CoV-2) ou J07BX03 (vaccins covid-19).

   Un ensemble de valeurs fixant les codes à utiliser conformément aux systèmes de codes établis dans la présente section est publié et régulièrement mis à jour par la Commission avec le soutien du réseau «Santé en ligne». L'ensemble de valeurs est étendu lorsque de nouveaux types de vaccins sont mis au point et utilisés.

▼M1

3. **Médicament vaccinal contre la COVID-19**

Systèmes de codes privilégiés (par ordre de préférence):

— Registre des médicaments de l'Union européenne pour les vaccins bénéficiant d'une autorisation à l'échelle de l'UE (numéros d'autorisation)

— Un registre mondial des vaccins, tel que celui qui pourrait être établi par l'Organisation mondiale de la santé

— Nom du médicament vaccinal dans les autres cas. Si le nom contient des espaces, il convient de remplacer celles-ci par un trait d'union (–).

Nom de l'ensemble de valeurs: vaccin.

À utiliser dans le certificat 1.

Exemple de code à utiliser, issu des systèmes de codes privilégiés: EU/1/20/1528 (Comirnaty). Exemple de nom de vaccin à utiliser comme code: Sputnik–V (correspondant à Sputnik V).

Un ensemble de valeurs fixant les codes à utiliser conformément aux systèmes de codes établis dans la présente section est publié et régulièrement mis à jour par la Commission avec le soutien du réseau «Santé en ligne».

Les vaccins sont codés à l'aide d'un code existant dans l'ensemble de valeurs publié, même si leur nom diffère d'un pays à l'autre. La raison en est qu'il n'existe pas encore de registre mondial des vaccins couvrant tous les vaccins actuellement utilisés. Exemple:

— Pour le vaccin «COVID-19 Vaccine Moderna Intramuscular Injection», qui est le nom du vaccin Spikevax au Japon, utiliser le code EU/1/20/1507 car c'est le nom de ce vaccin dans l'Union.

Si cela n'est pas possible ou pas souhaitable dans un cas particulier, un code distinct sera indiqué dans l'ensemble de valeurs publié.

▼M4

Si un pays qui utilise le certificat COVID numérique de l'UE décide de délivrer des certificats de vaccination aux participants à des essais cliniques en cours, le médicament vaccinal est codé suivant le modèle

CT*_identifiant-essai-clinique*

Lorsque l'essai clinique est inscrit au registre des essais cliniques de l'Union européenne, l'identifiant qui lui est attribué dans ce registre est utilisé. Dans les autres cas, les identifiants d'autres registres (tels que clinicaltrials.gov ou l'Australian New Zealand Clinical Trials Registry) peuvent être utilisés.

L'identifiant de l'essai clinique comporte un préfixe permettant d'identifier le registre dans lequel l'essai clinique est inscrit (EUCTR pour le registre des essais cliniques de l'Union européenne, NCT pour clinicaltrials.gov, ACTRN pour l'Australian New Zealand Clinical Trials Registry).

Lorsque la Commission a reçu, du comité de sécurité sanitaire, du Centre européen de prévention et de contrôle des maladies (ECDC) ou de l'Agence européenne des médicaments (EMA), des orientations concernant l'acceptation de certificats délivrés pour un vaccin contre la COVID-19 faisant l'objet d'essais cliniques, celles-ci sont publiées soit dans le document sur les ensembles de valeurs, soit séparément.

▼M1

4. **Titulaire de l'autorisation de mise sur le marché ou fabricant d'un vaccin contre la COVID-19**

Système de codes privilégié:

— Code d'organisation provenant de l'EMA (système SPOR pour les normes ISO IDMP)

— Un registre mondial des titulaires d'autorisations de mise sur le marché ou des fabricants de vaccins, tel que celui qui pourrait être établi par l'Organisation mondiale de la santé

— Nom de l'organisation dans les autres cas. Si le nom contient des espaces, il convient de remplacer celles-ci par un trait d'union (–).

À utiliser dans le certificat 1.

Exemple de code à utiliser, issu des systèmes de codes privilégiés: ORG-100001699 (AstraZeneca AB). Exemple de nom d'organisation à utiliser comme code: Sinovac–Biotech (correspondant à Sinovac Biotech).

Un ensemble de valeurs fixant les codes à utiliser conformément aux systèmes de codes établis dans la présente section est publié et régulièrement mis à jour par la Commission avec le soutien du réseau «Santé en ligne».

Les différentes filiales d'un même titulaire d'autorisation de mise sur le marché (AMM) ou d'un même fabricant utilisent un code existant dans l'ensemble de valeurs publié.

En règle générale, pour un même produit vaccinal, le code utilisé est celui qui fait référence au titulaire de l'autorisation de mise sur le marché dans l'Union, étant donné qu'il n'existe pas encore de registre des titulaires d'autorisations de mise sur le marché ou des fabricants de vaccins convenu au niveau international. Exemples:

— Pour l'organisation «Pfizer AG», qui est titulaire d'une AMM pour le vaccin «Comirnaty» utilisé en Suisse, utiliser le code ORG-100030215 qui fait référence à BioNTech Manufacturing GmbH car il s'agit du titulaire de l'AMM pour le Comirnaty dans l'Union.

— Pour l'organisation «Zuellig Pharma», qui est titulaire d'une AMM pour le vaccin «COVID-19 Vaccine Moderna» (Spikevax) utilisé aux Philippines, utiliser le code ORG-100031184 qui fait référence à Moderna Biotech Spain S.L car il s'agit du titulaire de l'AMM pour le Spikevax dans l'Union.

Si cela n'est pas possible ou pas souhaitable dans un cas particulier, un code distinct sera indiqué dans l'ensemble de valeurs publié.

▼M4

Si un pays qui utilise le certificat COVID numérique de l'UE décide de délivrer des certificats de vaccination aux participants à des essais cliniques en cours, le titulaire de l'autorisation de mise sur le marché ou le fabricant du vaccin est codé à l'aide de la valeur qui lui est attribuée dans l'ensemble de valeurs, si elle existe. Dans les autres cas, le titulaire de l'autorisation de mise sur le marché ou le fabricant du vaccin est codé en utilisant la règle décrite au point 3, Médicament vaccinal (CT_*identifiant-essai-clinique*).

▼M1

5. **Nombre dans une série de doses ainsi que nombre total de doses dans la série**

À utiliser dans le certificat 1.

Deux champs:

1) Nombre dans une série de doses de vaccin d'un vaccin contre la COVID-19 (N)

2) Nombre total de doses dans le schéma de vaccination (C)

5.1. *Schéma de primovaccination*

Lorsque la personne reçoit les doses du schéma de primovaccination, c'est-à-dire les injections de vaccin nécessaires pour offrir une protection suffisante à un stade initial, (C) correspond au nombre total de doses du schéma de primovaccination standard (par exemple, 1 ou 2, en fonction du type de vaccin administré). Cela inclut la possibilité d'utiliser une série abrégée (C = 1) lorsque le protocole de vaccination appliqué par un État membre prévoit l'administration d'une seule dose d'un vaccin à 2 doses aux personnes ayant été précédemment infectées par le SARS-CoV-2. Un schéma de primovaccination complet est donc indiqué par N/C = 1. Par exemple:

— 1/1 indiquerait l'achèvement d'un schéma de primovaccination à dose unique, ou l'achèvement d'un schéma de primovaccination consistant à administrer une seule dose d'un vaccin à 2 doses à une personne rétablie, conformément au protocole de vaccination appliqué par un État membre;

— 2/2 indiquerait l'achèvement d'un schéma de primovaccination à deux doses.

Lorsque le schéma de primovaccination est étendu, par exemple pour les personnes sévèrement immunodéprimées, ou lorsque l'intervalle recommandé entre les doses de primovaccination n'a pas été respecté, ces doses sont encodées comme des doses supplémentaires relevant de la section 5.2.

▼M2

5.2. *Doses de rappel*

Lorsqu'elles sont administrées à la suite du schéma de primovaccination, ces doses de rappel apparaissent dans les certificats correspondants comme suit:

— 2/1 indique l'administration d'une dose de rappel après l'achèvement d'un schéma de primovaccination à dose unique, ou l'administration d'une dose de rappel après l'achèvement d'un schéma de primovaccination consistant à administrer une seule dose d'un vaccin à deux doses à une personne rétablie, conformément au protocole de vaccination appliqué par un État membre. Ensuite, les doses (X) administrées à la suite de la première dose de rappel sont indiquées par (2+X)/(1) > 1 (3/1, par exemple),

— 3/3 indique l'administration d'une dose de rappel après l'achèvement d'un schéma de primovaccination à deux doses. Ensuite, les doses (X) administrées à la suite de la première dose de rappel sont indiquées par (3+X)/(3+X) = 1 (4/4, par exemple).

Les États membres mettent en œuvre les règles d'encodage énoncées dans la présente section au plus tard le 1er février 2022.

Les États membres délivrent à nouveau, automatiquement ou à la demande des personnes concernées, les certificats dans lesquels l'administration d'une dose de rappel à la suite d'un schéma de primovaccination à dose unique est encodée de telle sorte qu'elle ne peut pas être distinguée de l'achèvement du schéma de primovaccination.

▼M2

Aux fins de la présente annexe, les références aux «doses de rappel» doivent être entendues comme couvrant également les doses supplémentaires administrées afin de mieux protéger les individus qui développent des réponses immunitaires inadéquates à la suite de l'achèvement du schéma de primovaccination standard. Dans le cadre légal établi par le règlement (UE) 2021/953, les États membres peuvent prendre des mesures pour remédier à la situation des groupes vulnérables qui peuvent, en priorité, recevoir une dose supplémentaire. Par exemple, si un État membre décide d'administrer des doses supplémentaires uniquement à certains sous-groupes de la population, il peut choisir, conformément à l'article 5, paragraphe 1, du règlement (UE) 2021/953, de ne délivrer que sur demande, et non automatiquement, des certificats de vaccination indiquant que cette dose supplémentaire a été administrée. Dans ce cas, l'État membre informe les personnes concernées en conséquence, et leur indique qu'elles peuvent continuer à utiliser le certificat reçu après l'achèvement du schéma de primovaccination standard.

▼M1

6. **État membre ou pays tiers dans lequel le vaccin a été administré/le test a été effectué**

Système de codes privilégié: codes pays ISO 3166.

À utiliser dans les certificats 1, 2 et 3.

Contenu de l'ensemble de valeurs: la liste complète des codes à 2 lettres, disponible sous la forme d'un ensemble de valeurs défini dans la spécification FHIR (Fast Healthcare Interoperability Resources – Ressources d'interopérabilité rapide des soins de santé) (http://hl7.org/fhir/ValueSet/iso3166-1-2). Si la vaccination ou le test ont été effectués par une organisation internationale (comme le HCR ou l'OMS) et qu'aucune information sur le pays n'est disponible, il y a lieu d'utiliser un code pour l'organisation. Ces codes supplémentaires sont publiés et régulièrement mis à jour par la Commission avec le soutien du réseau "Santé en ligne".

7. **Type de test**

À utiliser dans le certificat 2, et dans le certificat 3 si le soutien à la délivrance de certificats de rétablissement sur la base de types de test autres que les TAAN est instauré par un acte délégué.

Les codes suivants sont utilisés:

Code	Affichage	Nom du système de code	URL du système de code	OID du système de code	Version du système de code
LP6464-4	Amplification des acides nucléiques avec détection de la sonde	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Immunodosage rapide	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Le code LP217198-3 (immunodosage rapide) est utilisé à la fois pour les tests rapides de détection d'antigènes et pour les tests antigéniques en laboratoire.

▼M1

8. **Nom du fabricant et dénomination commerciale du test utilisé (facultatifs pour les TAAN)**

À utiliser dans le certificat 2.

▼M4

Le contenu de l'ensemble de valeurs inclut la sélection d'un test de détection d'antigènes figurant sur la liste commune et actualisée des tests de détection d'antigènes pour le diagnostic de la COVID-19, établie sur la base de la recommandation du Conseil publiée au JO C 24 du 22.1.2021, p. 1. et approuvée par le comité de sécurité sanitaire. La liste est mise à jour par le JRC dans la base de données sur les dispositifs de diagnostic in vitro et les méthodes de dépistage de la COVID-19 à l'adresse suivante: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

Pour ce système de codes, il convient d'utiliser des champs pertinents tels que l'identifiant du dispositif de test, le nom du test et du fabricant, en respectant le format structuré du JRC disponible à l'adresse suivante: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Résultat du test**

À utiliser dans le certificat 2.

Les codes suivants sont utilisés:

Code	Affichage	Nom du système de code	URL du système de code	OID du système de code	Version du système de code
260415000	non détecté	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	détecté	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

ANNEXE III

STRUCTURE COMMUNE DE L'IDENTIFIANT UNIQUE DU CERTIFICAT

1. **Introduction**

Chaque certificat COVID numérique de l'UE comporte un identifiant unique du certificat (*unique certificate identifier* — UCI) qui favorise l'interopérabilité des DCC. L'UCI peut être utilisé pour vérifier le certificat. Les États membres sont chargés de la mise en œuvre de l'UCI. L'UCI est un moyen de vérifier l'authenticité du certificat et, le cas échéant, d'établir un lien vers un système d'enregistrement, par exemple, un système d'information sur la vaccination (*immunisation information system* — IIS). Cet identifiant doit également permettre aux États membres d'attester (sur papier et par voie numérique) que des personnes ont été vaccinées ou testées.

2. **Composition de l'identifiant unique du certificat**

L'UCI doit avoir une structure et un format communs facilitant l'interprétabilité des informations par l'homme et/ou par la machine et peut porter sur des éléments tels que l'État membre de vaccination, le vaccin lui-même et un identifiant propre à l'État membre. Cela assure aux États membres une certaine souplesse pour le formater, en respectant pleinement la législation en matière de protection des données. L'ordre des différents éléments suit une hiérarchie définie qui peut permettre de modifier les blocs à l'avenir sans nuire à l'intégrité structurelle.

Les solutions possibles pour la composition de l'UCI constituent un spectre dans lequel la modularité et l'interprétabilité par l'homme sont les deux principaux paramètres de diversification et une caractéristique fondamentale:

— modularité: la mesure dans laquelle le code est composé de blocs constitutifs distincts contenant des informations sémantiquement différentes,

— interprétabilité par l'homme: la mesure dans laquelle le code est porteur de sens ou peut être interprété par le lecteur humain,

— unique à l'échelle mondiale; l'identifiant du pays ou de l'autorité est bien géré; et chaque pays (autorité) est censé bien gérer son segment de l'espace de noms en ne recyclant jamais les identifiants et en ne les réassignant pas. La combinaison de ces éléments garantit que chaque identifiant est unique à l'échelle mondiale.

▼M1

3. **Exigences générales**

En ce qui concerne l'UCI, les exigences générales à respecter sont les suivantes:

1) Jeu de caractères: seuls les caractères alphanumériques US-ASCII majuscules ("A" à "Z", "0" à "9") sont autorisés, avec des caractères spéciaux supplémentaires séparateurs selon la RFC3986 ([1]), à savoir {'/','#',':'}.

2) Longueur maximale: pour les concepteurs, l'objectif devrait être une longueur de 27 à 30 caractères ([2]).

3) Préfixe de version: fait référence à la version du schéma UCI. Le préfixe de version est "01" pour la présente version du document; le préfixe de version est composé de deux chiffres.

([1]) rfc3986 (ietf.org)

([2]) Pour la mise en œuvre avec des codes QR, les États membres pourraient envisager d'utiliser un jeu supplémentaire de caractères d'une longueur maximale totale de 72 caractères (y compris les 27 à 30 caractères de l'identifiant proprement dit) pour transmettre d'autres informations. Il appartient aux États membres de définir les spécifications de ces informations.

▼M1

4) Préfixe du pays: le code pays est spécifié par la norme ISO 3166-1. Les codes plus longs [c'est-à-dire 3 caractères et plus (par exemple, "UNHCR")] sont réservés à une utilisation future.

5) Suffixe de code/Somme de contrôle.

5.1. Les États membres peuvent utiliser une somme de contrôle lorsqu'une transmission, une transcription (humaine) ou une autre forme d'altération peuvent se produire (c'est-à-dire en cas d'utilisation en version imprimée).

5.2. La somme de contrôle n'est pas utilisée pour valider le certificat et ne fait pas techniquement partie de l'identifiant, mais sert à vérifier l'intégrité du code. Cette somme de contrôle est le résumé ISO 7812-1 (LUHN-10) ([1]) de l'UCI entier au format de transport filaire/numérique. La somme de contrôle est séparée du reste de l'UCI par le caractère "#".

La compatibilité rétrospective est assurée: les États membres qui, au fil du temps, modifient la structure de leurs identifiants (dans la version principale, actuellement fixée à v1) veillent à ce que deux identifiants, quels qu'ils soient, qui sont identiques se rapportent au même certificat ou à la même déclaration de vaccination. En d'autres termes, les États membres ne peuvent pas recycler les identifiants.

▼B

4. **Options en matière d'identifiants uniques pour les certificats de vaccination**

Les lignes directrices du réseau «Santé en ligne» concernant les certificats de vaccination vérifiables et les éléments d'interopérabilité de base ([2]) offrent aux États membres et à d'autres parties diverses options qui peuvent coexister entre différents États membres. Les États membres peuvent déployer ces diverses options dans différentes versions du schéma UCI.

([1]) L'algorithme de Luhn mod N est une extension de l'algorithme de Luhn (aussi appelé algorithme mod 10) utilisé pour les codes numériques, qui sert par exemple à calculer les sommes de contrôle des numéros de cartes de crédit. L'extension permet à l'algorithme de fonctionner avec des séquences de valeurs dans n'importe quelle base (en l'occurrence, des caractères alphabétiques).

([2]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

▼B

ANNEXE IV

GOUVERNANCE DES CERTIFICATS DE CLÉ PUBLIQUE

1. **Introduction**

L'échange sécurisé et fiable de clés de signature pour les certificats COVID numériques de l'UE (*Digital COVID certificates*, DCC) entre les États membres s'effectue par l'intermédiaire du service passerelle des certificats COVID numériques de l'UE (*Digital COVID Certificate Gateway,* DCCG), qui sert de répertoire central des clés publiques. Le DCCG donne aux États membres les moyens de publier les clés publiques correspondant aux clés privées qu'ils utilisent pour signer des certificats COVID numériques. Les États membres utilisateurs peuvent avoir recours au DCCG pour obtenir en temps voulu des clés publiques actualisées. Par la suite, le DCCG pourra être étendu pour permettre l'échange d'informations supplémentaires fiables fournies par les États membres, telles que des règles de validation concernant les DCC. Le modèle de confiance du cadre DCC est une infrastructure à clé publique (ICP). Chaque État membre a une ou plusieurs autorités nationales de signature de certificats (CSCA), dont les certificats ont une durée de vie relativement longue. Selon la décision de l'État membre, il peut s'agir d'une CSCA identique à celle utilisée pour les documents de voyage lisibles par machine ou d'une autorité différente. La CSCA délivre des certificats de clé publique pour les signataires de documents nationaux (c'est-à-dire les signataires des DCC), dont la durée de vie est brève, qui sont appelés certificats de signataire de documents (DSC). La CSCA joue un rôle d'ancre de confiance, de sorte que les États membres utilisateurs peuvent utiliser le certificat CSCA pour valider l'authenticité et l'intégrité des DSC qui changent régulièrement. Une fois la validation effectuée, les États membres peuvent fournir ces certificats (ou uniquement les clés publiques qu'ils contiennent) à leurs applications de validation des DCC. Outre les CSCA et les DSC, le DCCG utilise également les ICP pour authentifier les transactions, signer les données, comme base d'authentification et comme moyen de garantir l'intégrité des canaux de communication entre les États membres et le DCCG.

Les signatures numériques peuvent être utilisées pour garantir l'intégrité et l'authenticité des données. Les ICP établissent la confiance en associant des clés publiques à des identités vérifiées (ou des émetteurs). Cela est nécessaire pour permettre aux autres participants de vérifier l'origine des données et l'identité de l'interlocuteur et de décider s'ils peuvent leur accorder leur confiance. Le DCCG fait appel à des certificats de clé publique multiples à des fins d'authenticité. La présente annexe définit les certificats de clé publique utilisés et la manière dont ils doivent être conçus pour permettre une large interopérabilité entre les États membres. Elle fournit davantage de détails sur les certificats de clé publique nécessaires ainsi que des orientations sur les modèles de certificats et les périodes de validité pour les États membres qui souhaitent avoir leur propre CSCA. Étant donné que les DCC doivent être vérifiables pendant un laps de temps déterminé (à compter de la délivrance, expiration après un certain délai), il est nécessaire de définir un modèle de vérification pour toutes les signatures apposées sur les certificats de clé publique et les DCC.

2. **Terminologie**

Le tableau suivant contient les abréviations et la terminologie utilisées dans la présente annexe.

Terme	Définition
Certificat	Ou certificat de clé publique. Certificat X.509 v3 contenant la clé publique d'une entité

▼B

Terme	Définition
CSCA	Autorité nationale de signature de certificats
DCC	Certificat COVID numérique de l'UE. Document numérique signé contenant des informations sur la vaccination, les tests ou le rétablissement
DCCG	Service passerelle du certificat COVID numérique de l'UE. Système utilisé pour l'échange de DSC entre les États membres.
$DCCG_{TA}$	Certificat d'ancre de confiance du DCCG. La clé privée correspondante est utilisée pour signer la liste de tous les certificats CSCA hors ligne.
$DCCG_{TLS}$	Certificat de serveur TLS (*Transport Layer Security* — Sécurité de la couche de transport) du DCCG.
DSC	Certificat de signataire de documents. Certificat de clé publique de l'autorité de signature des documents d'un État membre (par exemple, un système autorisé à signer des DCC). Ce certificat est délivré par la CSCA de l'État membre.
ECDSA	Algorithme de signature numérique à courbe elliptique. Algorithme de signature cryptographique reposant sur les courbes elliptiques
État membre	État membre de l'Union européenne
mTLS	TLS mutuels. Protocole de sécurité de la couche de transport avec authentification mutuelle
NB	Système d'arrière-plan national d'un État membre
NB_{CSCA}	Certificat CSCA d'un État membre (il peut y en avoir plus d'un)
NB_{TLS}	Certificat d'authentification client TLS d'un système d'arrière-plan national
NB_{UP}	Certificat utilisé par un système d'arrière-plan national pour signer des paquets de données qui sont téléversés dans le DCCG
ICP	Infrastructure à clé publique. Modèle de confiance reposant sur les certificats de clé publique et les autorités de certification
RSA	Algorithme de cryptographie asymétrique reposant sur la factorisation des nombres entiers, utilisé pour les signatures numériques ou le chiffrement asymétrique

3. **Flux de communication et services de sécurité du DCCG**

La présente section donne un aperçu des flux de communication et des services de sécurité dans le système du DCCG. Elle définit également les clés et certificats utilisés pour protéger la communication, les informations téléversées, les DCC et une *trust list* signée qui contient tous les certificats CSCA enrôlés. Le DCCG fonctionne comme une plateforme de données qui permet l'échange de paquets de données signés pour les États membres.

▼B

Les paquets de données téléversés sont fournis par le DCCG «en l'état», ce qui signifie que le DCCG n'ajoute ni ne supprime aucun DSC des paquets qu'il reçoit. Le système d'arrière-plan national (*national backend* — NB) des États membres est en mesure de vérifier l'intégrité et l'authenticité de bout en bout des données téléversées. En outre, les systèmes d'arrière-plan nationaux et le DCCG utiliseront l'authentification mutuelle TLS pour établir une connexion sécurisée. Ces mesures s'ajoutent aux signatures figurant dans les données échangées.

3.1. *Authentification et établissement de la connexion*

Le DCCG utilise le protocole TLS avec authentification mutuelle pour établir un canal crypté authentifié entre le système d'arrière-plan national de l'État membre (NB) et l'environnement du service passerelle. Par conséquent, le DCCG détient un certificat de serveur TLS, dit «$DCCG_{TLS}$», et les systèmes d'arrière-plan nationaux détiennent un certificat client TLS — appelé NB_{TLS}. Les modèles de certificat sont fournis à la *section 5*. Tous les systèmes d'arrière-plan nationaux peuvent fournir leur propre certificat TLS. Ce certificat sera explicitement placé sur liste blanche et il peut par conséquent être délivré par une autorité de certification publique de confiance (par exemple, une autorité de certification qui respecte les exigences de base du CA/Browser Forum), par une autorité nationale de certification ou être autosigné. Chaque État membre est responsable de ses données nationales et de la protection de la clé privée utilisée pour établir la connexion avec le DCCG. L'approche «Apporter son propre certificat» requiert une procédure d'enregistrement et d'identification bien définie, ainsi que des procédures de révocation et de renouvellement, qui sont décrites aux sections 4.1, 4.2 et 4.3. Le DCCG utilise une liste blanche sur laquelle les certificats TLS des NB sont inscrits lorsque leur enregistrement a été effectué avec succès. Seuls les NB qui s'authentifient au moyen d'une clé privée correspondant à un certificat figurant sur la liste blanche peuvent établir une connexion sécurisée avec le DCCG. Le DCCG utilisera également un certificat TLS qui permet aux NB de vérifier qu'ils établissent effectivement une connexion avec le «véritable» DCCG et non avec une entité malveillante qui se fait passer pour le DCCG. Le certificat du DCCG sera fourni aux NB après un enregistrement effectué avec succès. Le certificat $DCCG_{TLS}$ sera délivré par une autorité de certification publique de confiance (incluse dans tous les principaux navigateurs). Il incombe aux États membres de vérifier que leur connexion au DCCG est sécurisée (par exemple, en vérifiant l'empreinte digitale du certificat $DCCG_{TLS}$ du serveur auquel ils sont connectés par rapport à celle qui a été fournie après l'enregistrement).

3.2. *Autorités nationales de signature de certificats et modèle de validation*

Les États membres participant au cadre DCCG doivent faire appel à une CSCA pour délivrer les DSC. Un État membre peut avoir plusieurs CSCA (par exemple, en cas de décentralisation régionale). Chaque État membre peut soit avoir recours aux autorités de certification existantes, soit mettre en place une autorité de certification spécifique (éventuellement autosignée) pour le système de DCC.

Les États membres doivent présenter leur(s) certificat(s) CSCA à l'exploitant du DCCG lors de la procédure officielle d'enrôlement. Après l'enregistrement réussi de l'État membre (voir la section 4.1 pour plus de détails), l'exploitant du DCCG mettra à jour une *trust list* signée contenant tous les certificats CSCA actifs dans le cadre du DCC. L'exploitant du DCCG utilisera une paire de clés asymétriques dédiée pour signer la *trust list* et les certificats dans un environnement hors ligne. La clé privée ne sera pas stockée dans le système du DCCG en ligne, afin qu'un attaquant ne puisse pas compromettre la *trust list* si le système en ligne est compromis. Le certificat d'ancre de confiance correspondant $DCCG_{TA}$ sera fourni aux systèmes d'arrière-plan nationaux lors du processus d'enrôlement.

▼B

Les États membres peuvent obtenir la *trust list* auprès du DCCG pour leurs procédures de vérification. La CSCA est définie comme l'autorité de certification (CA) qui délivre des DSC, c'est pourquoi les États membres qui utilisent une hiérarchie d'autorités de certification à plusieurs niveaux (par exemple, CA racine — > CSCA — > DSC) doivent fournir l'autorité de certification subordonnée qui délivre les DSC. Dans ce cas, si un État membre fait appel à une autorité de certification existante, le système de DCC fera abstraction de tout ce qui se trouve au-dessus de la CSCA et ne placera sur la liste blanche que la CSCA en tant qu'ancre de confiance (même s'il s'agit d'une CA subordonnée). C'est le modèle de l'OACI, qui n'autorise que 2 niveaux — une CSCA «racine» et un DSC «feuille» signé par cette seule CSCA.

Si un État membre exploite sa propre CSCA, il est responsable du fonctionnement sécurisé et de la gestion des clés de cette autorité. La CSCA joue le rôle d'ancre de confiance pour les DSC et, par conséquent, la protection de la clé privée de la CSCA est essentielle pour l'intégrité de l'environnement du DCC. Le modèle de vérification dans l'ICP des DCC est le modèle *shell*, qui prévoit que tous les certificats présents dans la validation du chemin du certificat doivent être valables à un moment précis (c'est-à-dire au moment de la validation de la signature). Par conséquent, les restrictions suivantes s'appliquent:

— la CSCA ne doit pas délivrer de certificats dont la durée de validité est supérieure à celle du certificat de la CA lui-même;

— le signataire de documents ne doit pas signer de documents dont la durée de validité est supérieure à celle du DSC proprement dit;

— les États membres qui exploitent leur propre CSCA doivent définir des périodes de validité pour leur CSCA et tous les certificats délivrés, et ils doivent prendre soin de renouveler les certificats.

La section 4.2 contient des recommandations concernant les périodes de validité.

3.3. *Intégrité et authenticité des données téléversées*

Les systèmes d'arrière-plan nationaux peuvent utiliser le DCCG pour téléverser et télécharger des paquets de données signés numériquement après une authentification mutuelle réussie. Au début, ces paquets de données contiennent les DSC des États membres. La paire de clés utilisée par le système d'arrière-plan national pour la signature numérique des paquets de données téléversés dans le système du DCCG est appelée «paire de clés du système d'arrière-plan national pour signature de téléversement» et on désigne le certificat de clé publique correspondant par l'abréviation NB_{UP}. Chaque État membre apporte son propre certificat NB_{UP}, qui peut être autosigné ou délivré par une autorité de certification existante, telle qu'une autorité de certification publique (c'est-à-dire une autorité de certification qui délivre des certificats conformément aux exigences de base du CA/Browser Forum). Le certificat NB_{UP} doit être différent de tous les autres certificats utilisés par l'État membre (certificats CSCA, client TLS ou DSC).

Les États membres doivent fournir le certificat de téléversement à l'exploitant du DCCG au cours de la procédure d'enregistrement initiale (voir la section 4.1 pour plus de détails). Chaque État membre est responsable de ses données nationales et doit assurer la protection de la clé privée utilisée pour signer les téléversements.

D'autres États membres peuvent vérifier les paquets de données signés à l'aide des certificats de téléversement fournis par le DCCG. Le DCCG vérifie l'authenticité et l'intégrité des données téléversées au moyen du certificat de téléversement du NB avant que les données ne soient fournies aux autres États membres.

▼B

3.4. *Exigences relatives à l'architecture technique du DCCG*

Les exigences relatives à l'architecture technique du DCCG sont les suivantes:

— le DCCG utilise l'authentification TLS mutuelle pour établir une connexion cryptée authentifiée avec les NB. Par conséquent, le DCCG tient à jour une liste blanche de certificats clients NB_{TLS} enregistrés,

— le DCCG utilise deux certificats numériques ($DCCG_{TLS}$ et $DCCG_{TA}$) avec deux paires de clés distinctes. La clé privée de la paire de clés $DCCG_{TA}$ est conservée hors ligne (et non sur les composants en ligne du DCCG),

— le DCCG tient à jour une *trust list* des certificats NB_{CSCA} signée avec la clé privée $DCCG_{TA}$,

— le chiffrement utilisé doit satisfaire aux exigences de la section 5.1.

4. **Gestion du cycle de vie des certificats**

4.1. *Enregistrement des systèmes d'arrière-plan nationaux*

Les États membres doivent s'enregistrer auprès de l'exploitant du DCCG pour participer au système du DCCG. La présente section décrit la procédure technique et opérationnelle qui doit être suivie pour enregistrer un système d'arrière-plan national.

L'exploitant du DCCG et l'État membre doivent échanger des informations sur les personnes à contacter pour des questions techniques sur le processus d'enrôlement. Il est présumé que ces personnes de contact bénéficient d'une habilitation de leur État membre et que leur identification/authentification est effectuée par d'autres canaux. Par exemple, l'authentification peut être réalisée lorsque la personne chargée des contacts techniques d'un État membre fournit par courriel les certificats sous forme de fichiers cryptés par mot de passe et communique par téléphone à l'exploitant du DCCG le mot de passe correspondant. D'autres canaux sécurisés définis par l'exploitant du DCCG peuvent également être utilisés.

L'État membre doit fournir trois certificats numériques au cours du processus d'enregistrement et d'identification:

— le certificat TLS de l'État membre NB_{TLS}

— le certificat de téléversement de l'État membre NB_{UP}

— le(s) certificat(s) CSCA de l'État membre NB_{CSCA}

Tous les certificats fournis doivent respecter les exigences définies à la section 5. L'exploitant du DCCG vérifiera que le certificat fourni satisfait aux exigences de la section 5. Après l'identification et l'enregistrement, l'exploitant du DCCG:

— ajoute le(s) certificat(s) NB_{CSCA} à la *trust list* signée au moyen de la clé privée correspondant à la clé publique $DCCG_{TA}$;

— ajoute le certificat NB_{TLS} à la liste blanche du point de terminaison TLS du DCCG;

— ajoute le certificat NB_{UP} au système du DCCG;

— fournit le certificat de clé publique $DCCG_{TA}$ et $DCCG_{TLS}$ à l'État membre.

▼B

4.2. *Autorités de certification, périodes de validité et renouvellement*

Si un État membre souhaite exploiter sa propre CSCA, les certificats CSCA peuvent être des certificats autosignés. Ils jouent le rôle d'ancre de confiance de l'État membre et, par conséquent, l'État membre doit prendre des mesures robustes pour protéger la clé privée correspondant à la clé publique du certificat CSCA. Il est recommandé aux États membres d'utiliser un système hors ligne pour leur CSCA, c'est-à-dire un système informatique qui n'est connecté à aucun réseau. L'accès au système doit être soumis à un contrôle multiple (par exemple, selon le principe des quatre yeux). Après la signature des DSC, des contrôles opérationnels doivent être appliqués et le système qui détient la clé CSCA privée doit être stocké en toute sécurité et faire l'objet de contrôles d'accès rigoureux. Des modules de sécurité matériels ou des cartes intelligentes peuvent être utilisés pour renforcer la protection de la clé privée CSCA. Les certificats numériques prévoient une période de validité qui impose de respecter le renouvellement des certificats. Le renouvellement est nécessaire pour utiliser de nouvelles clés cryptographiques et adapter les tailles de clés lorsque de nouveaux progrès dans le domaine du calcul ou de nouvelles attaques menacent la sécurité de l'algorithme de cryptographie utilisé. Le modèle *shell* s'applique (voir section 3.2).

Sur la base d'une durée de validité d'un an pour les certificats COVID numériques, les durées de validité recommandées sont les suivantes:

— CSCA: 4 ans

— DSC: 2 ans

— téléversement: 1-2 ans

— authentification du client TLS: 1-2 ans

Pour que le renouvellement puisse avoir lieu en temps voulu, les périodes d'utilisation recommandées pour les clés privées sont les suivantes:

— CSCA: 1 an

— DSC: 6 mois

Les États membres doivent créer de nouveaux certificats de téléversement et de nouveaux certificats TLS en temps voulu, par exemple un mois avant la date d'expiration, afin de garantir un fonctionnement harmonieux. Les certificats CSCA et les DSC devraient être renouvelés au moins un mois avant que l'utilisation de la clé privée ne prenne fin (en tenant compte des procédures opérationnelles nécessaires). Les États membres doivent fournir à l'exploitant du DCCG des certificats CSCA, des certificats de téléversement et des certificats TLS actualisés. Les certificats périmés doivent être retirés de la liste blanche et de la *trust list*.

Les États membres et l'exploitant du DCCG doivent assurer le suivi de la validité de leurs propres certificats. Il n'existe pas d'entité centrale qui assure le suivi de la validité des certificats et en informe les participants.

▼B

4.3. *Révocation de certificats*

En général, les certificats numériques peuvent être révoqués par leur autorité de certification émettrice au moyen des listes de révocation des certificats ou du protocole de vérification des certificats en ligne (*Online Certificate Status Protocol Responder* — service OCSP). Les CSCA pour le système de DCC devraient fournir des listes de révocation de certificats (CRL). Même si ces CRL ne sont pas utilisées actuellement par les autres États membres, elles devaient être intégrées en prévision d'applications futures. Si une CSCA décide de ne pas fournir de CRL, les DSC de cette CSCA devront être renouvelés lorsque les CRL deviendront obligatoires. Pour la validation des DSC, les vérificateurs devraient utiliser les CRL et non le service OCSP. Il est recommandé que le système d'arrière-plan national procède à la validation nécessaire des DSC téléchargés à partir du DCCG et ne transmette aux validateurs de DCC nationaux qu'une série de DSC dignes de confiance et validés. Les validateurs des DCC ne devraient pas effectuer de contrôle de révocation sur les DSC dans le cadre de leur processus de validation. Cela correspond, notamment, au souci de protéger la vie privée des titulaires de DCC en prévenant tout risque que l'utilisation d'un DSC donné puisse être surveillée par le service OCSP qui lui est associé.

Les États membres peuvent retirer leurs DSC du DCCG de leur propre initiative en utilisant des certificats de téléversement et des certificats TLS valides. Lorsqu'un DSC est supprimé, tous les DCC délivrés avec ce DSC deviendront invalides lorsque les États membres consulteront les listes de DSC actualisées. La protection des clés privées correspondant aux DSC est cruciale. Les États membres doivent informer l'exploitant du DCCG lorsqu'ils doivent révoquer des certificats de téléversement ou TLS, par exemple en raison d'une compromission du système d'arrière-plan national. L'exploitant du DCCG peut alors retirer la confiance accordée au certificat concerné, par exemple en le supprimant de la liste blanche TLS. L'exploitant du DCCG peut supprimer les certificats de téléversement de la base de données DCCG. Les paquets signés avec la clé privée correspondant à ce certificat de téléversement deviendront invalides lorsque les systèmes d'arrière-plan nationaux retireront la confiance accordée au certificat de téléversement révoqué. Si un certificat CSCA doit être révoqué, les États membres doivent en informer l'exploitant du DCCG ainsi que les autres États membres avec lesquels ils entretiennent des relations de confiance. L'exploitant du DCCG publiera une nouvelle *trust list* sur laquelle le certificat concerné ne figurera plus. Tous les DSC émis par cette CSCA deviendront invalides lorsque les États membres mettront à jour leur magasin de confiance d'arrière-plan national. Si le certificat $DCCG_{TLS}$ ou le certificat $DCCG_{TA}$ doit être révoqué, l'exploitant du DCCG et les États membres doivent collaborer pour établir une nouvelle connexion TLS de confiance ainsi qu'une nouvelle *trust list*.

5. **Modèles de certificats**

La présente section énonce des exigences et fournit des orientations en ce qui concerne la cryptographie et établit également des exigences relatives aux modèles de certificat. Pour ce qui concerne les certificats DCCG, la présente section définit les modèles de certificats.

5.1. *Exigences cryptographiques*

Les algorithmes de cryptographie et les suites cryptographiques TLS seront choisis sur la base des recommandations en vigueur de l'Office fédéral allemand de la sécurité de l'information (BSI) ou du SOG-IS.Ces recommandations et celles d'autres institutions et organismes de normalisation sont similaires. Les recommandations figurent dans les orientations techniques TR 02102-1 et TR 02102-2 ([20]) ([1]) ou dans les mécanismes cryptographiques approuvés du SOG-IS ([2]).

([1]) BSI - Technical Guidelines TR-02102 (bund.de)
([2]) SOG-IS - Supporting documents (sogis.eu)

▼B

5.1.1. Exigences relatives au DSC

Les exigences prévues à l'annexe I, section 3.2.2 sont applicables. Par conséquent, il est vivement recommandé aux signataires de documents d'utiliser l'algorithme de signature numérique à courbe elliptique (ECDSA) avec la courbe NIST-p-256 (telle que définie à l'appendice D de la norme FIPS PUB 186-4). Les autres courbes elliptiques ne sont pas prises en charge. En raison des contraintes d'espace imposées par le DCC, les États membres ne devraient pas utiliser le RSA-PSS, même s'il est autorisé en tant qu'algorithme de secours. Si les États membres ont recours au RSA-PSS, ils doivent utiliser un modulus d'une taille de 2048 ou 3072 bits au maximum. SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits doit être utilisé comme fonction de hachage cryptographique (voir ISO/IEC 10118-3: 2004) pour la signature du DSC.

5.1.2. Exigences relatives aux certificats TLS, de téléversement et CSCA

Pour les certificats numériques et les signatures cryptographiques dans le contexte du DCCG, les principales exigences relatives aux algorithmes cryptographiques et à la longueur des clés sont résumées dans le tableau suivant (à partir de 2021):

Algorithme de signature	Taille de la clé	Fonction de hachage
ECDSA	Min. 250 bits	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits
RSA-PSS (bourrage recommandé) RSA-PKCS # 1 v1.5 (versions antérieures pour bourrage)	Min. 3000 bits modulus RSA *n* avec exposant public e > 2 ^ 16	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits
DSA	Min. 3000 bits nombre premier p, 250 bits clé q	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits

La courbe elliptique recommandée pour l'ECDSA est la NIST-p-256 car elle est largement utilisée.

5.2. *Certificat CSCA (NB_{CSCA})*

Le tableau suivant fournit des indications sur le modèle de certificat NB_{CSCA} si un État membre décide d'exploiter sa propre CSCA pour le système de DCC.

Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>*,**c=<État membre exploitant la CSCA>**
Key usage	**certificate signing,***CRL signing* (au minimum)
Basic Constraints	**CA = true, path length constraints = 0**

Le nom du sujet doit être non vide et unique dans l'État membre considéré. Le code pays (c) doit correspondre à l'État membre qui utilisera ce certificat CSCA. Le certificat doit contenir un identifiant de clé du sujet (SKI) unique conforme à la RFC 5280 ([1]).

([1]) rfc5280 (ietf.org).

▼B

5.3. *Certificat de signataire de documents (DSC)*

Le tableau suivant fournit des orientations sur le DSC. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Serial Number	**numéro de série unique**
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>*,**c=<État membre utilisant ce DSC>**
Key Usage	**digital signature** (au minimum)

Le DSC doit être signé avec la clé privée correspondant à un certificat CSCA utilisé par l'État membre.

Les extensions suivantes doivent être utilisées:

— le certificat doit contenir un identifiant de clé de l'autorité (AKI) correspondant à l'identifiant de clé du sujet (SKI) du certificat de la CSCA émettrice,

— le certificat doit contenir un identifiant de clé du sujet (SKI) unique conforme à la RFC 5280 ([1]).

En outre, le certificat doit contenir l'extension du point de distribution de la CRL qui renvoie à la liste de révocation de certificats (CRL) fournie par la CSCA qui a émis le DSC.

Le DSC peut contenir une extension EKU (*extended key usage* — utilisation étendue de la clé) avec zéro ou plusieurs identifiants de la politique d'utilisation des clés qui limitent les types de HCERT que ce certificat est autorisé à vérifier. Si un ou plusieurs identifiants sont présents, les vérificateurs vérifient l'utilisation de la clé par rapport au HCERT stocké. Les valeurs d'utilisation étendue de la clé suivantes sont définies à cet effet:

Champ	Valeur
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pour les émetteurs «tests»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pour les émetteurs «vaccination»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pour les émetteurs «rétablissement»

En l'absence d'extension d'utilisation de la clé (c'est-à-dire pas d'extension ou zéro extension), ce certificat peut être utilisé pour valider tout type de HCERT. D'autres identifiants de politique d'utilisation étendue de la clé pertinents utilisés avec la validation des HCERT peuvent être définis par d'autres documents.

5.4. *Certificats de téléversement (NB_{UP})*

Le tableau suivant fournit des orientations pour le certificat de téléversement du système d'arrière-plan national. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

([1]) rfc5280 (ietf.org).

▼B

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,***c=<État membre utilisant ce certificat de téléversement>**
Key Usage	**digital signature** (au minimum)

5.5. *Certificat d'authentification client TLS du système d'arrière-plan national (NB_{TLS})*

Le tableau suivant fournit des orientations pour le certificat d'authentification client TLS du système d'arrière-plan national. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,***c=<État membre sur le NB>**
Key Usage	**digital signature** (au minimum)
Extended key usage	client authentication (1.3.6.1.5.5.7.3.2)

Le certificat peut également contenir le *server authentication (1.3.6.1.5.5.7.3.1)* de l'utilisation étendue de la clé, mais ce n'est pas obligatoire.

5.6. *Certificat de signature de la trust list ($DCCG_{TA}$)*

Le tableau suivant définit le certificat d'ancre de confiance du DCCG.

Champ	Valeur
Subject	**cn = Digital Green Certificate Gateway** ([1]), **o=<Prestataire>, c=<pays>**
Key Usage	**digital signature** (au minimum)

5.7. *Certificats de serveur TLS du DCCG ($DCCG_{TLS}$)*

Le tableau suivant définit le certificat TLS du DCCG.

Champ	Valeur
Subject	cn=<FQDN ou adresse IP du DCCG>, o=<Prestataire>, c= <pays>
SubjectAltName	dNSName: <Nom DCCG DNS> ou iPAddress: <adresse IP DCCG>
Key Usage	**digital signature** (au minimum)
Extended key usage	server authentication (1.3.6.1.5.5.7.3.1)

([1]) Le terme «Digital Green Certificate» au lieu de «EU Digital COVID Certificate» a été conservé dans ce contexte, car c'est cette terminologie qui a été codifiée et déployée dans le certificat avant que les colégislateurs ne s'accordent sur un nouveau terme.

▼B

Le certificat peut également contenir le *client authentication (1.3.6.1.5.5.7.3.2)* de l'utilisation étendue de la clé, mais ce n'est pas obligatoire.

Le certificat TLS du DCCG doit être délivré par une autorité de certification de confiance publique (incluse dans tous les principaux navigateurs et systèmes d'exploitation, conformé

▼M1

ANNEXE V

SCHÉMA JAVASCRIPT OBJECT NOTATION (JSON)

1. **Introduction**

La présente annexe établit la structure technique des données pour les certificats COVID numériques de l'UE (DCCUE), représentés sous la forme d'un schéma JSON. Le document fournit des instructions spécifiques relatives aux différents champs de données.

2. **Emplacement et versions du schéma JSON**

Le schéma JSON officiel faisant autorité pour le DCCUE est disponible à l'adresse suivante: https://github.com/ehn-dcc-development/ehn-dcc-schema. D'autres emplacements ne font pas autorité, mais peuvent être utilisés pour préparer les révisions à venir.

Par défaut, la version en cours décrite dans la présente annexe et supportée par tous les pays qui émettent actuellement des certificats se trouve à l'URL indiquée.

La prochaine version qui, à une date déterminée, devra être supportée par tous les pays, se trouve à l'URL indiquée via le marquage des versions (*version tagging*), une description plus précise est fournie dans le fichier Readme.

▼M3

3. **Structures communes et exigences générales**

Le certificat COVID numérique de l'UE n'est pas délivré si, en raison de l'absence d'informations, tous les champs de données ne peuvent pas être correctement complétés conformément à la présente spécification. **Cela ne doit pas être interprété comme remettant en cause l'obligation des États membres de délivrer des certificats COVID numériques de l'UE.**

Dans tous les champs, il est possible d'indiquer les informations au moyen de la série complète de caractères UNICODE 13.0 encodés en UTF-8, sauf en cas de restriction spécifique à des ensembles de valeurs ou à des ensembles de caractères plus réduits.

La structure commune est la suivante:

"JSON":{

"ver":<information sur la version>,

"nam":{

<informations sur le nom de la personne>

},

"dob":<date de naissance>,

"v" ou "t" ou "r":[

{<informations sur la dose de vaccin ou sur le test de dépistage ou de rétablissement, une seule entrée>}

]

}

Des informations détaillées sur les différents groupes et champs sont fournies dans les points ci-après.

Lorsque les règles indiquent qu'un champ doit être ignoré, cela signifie que son contenu doit être vide et que ni le nom ni la valeur du champ ne sont autorisés dans le contenu.

▼M3

3.1. *Version*

Il y a lieu de fournir des informations sur la version. La gestion des versions s'effectue selon Semantic Versioning (semver: https://semver.org). En production, il s'agit de l'une des versions officiellement publiées (en cours ou officiellement publiées antérieurement). Pour plus de détails, voir le point Emplacement du schéma JSON.

Identifiant du champ	Nom du champ	Instructions
ver	Version de schéma	Correspond à l'identifiant de la version du schéma utilisée pour produire l'EUDCC. Exemple: "ver":"1.3.0"

3.2. *Nom et date de naissance de la personne*

Le nom de la personne est le nom officiel complet de la personne, correspondant au nom indiqué sur les documents de voyage. L'identifiant de la structure est *nam*. Exactement 1 (un) nom de personne est indiqué.

Identifiant du champ	Nom du champ	Instructions
nam/fn	Nom(s)	Nom(s) du titulaire Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, tous les noms y étant inclus. S'il y a plusieurs noms, ils sont séparés par une espace. Les noms composés comprenant des traits d'union ou des caractères similaires ne doivent toutefois pas être modifiés. Exemples: "fn":"Musterfrau-Gößinger" "fn":"Musterfrau-Gößinger Müller"
nam/fnt	Nom(s) normalisé(s)	Nom(s) du titulaire translitteré(s) suivant la même convention que celle utilisée pour les documents de voyage lisibles par machine du titulaire (par exemple, les règles définies dans le document ICAO 9303, partie 3). Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, comportant uniquement les caractères A-Z et <. Longueur maximale: 80 caractères (selon la spécification du document ICAO 9303). Exemples: "fnt":"MUSTERFRAU<GOESSINGER" "fnt":"MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Prénom(s)	Prénom(s) du titulaire. Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, tous les prénoms y étant inclus. S'il y a plusieurs prénoms, ils sont séparés par une espace. Exemple: "gn":"Isolde Erika"

▼M3

Identifiant du champ	Nom du champ	Instructions
nam/gnt	Prénom(s) normalisé(s)	Prénom(s) du titulaire translittéré(s) suivant la même convention que celle utilisée pour les documents de voyage lisibles par machine du titulaire (par exemple, les règles définies dans le document ICAO 9303, partie 3). Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, comportant uniquement les caractères A-Z et <. Longueur maximale: 80 caractères Exemple: "gnt":"ISOLDE<ERIKA"
dob	Date de naissance	Date de naissance du titulaire du DCC Date complète ou partielle sans heure, plage limitée à la période comprise entre le 1900-01-01 et le 2099-12-31. Exactement 1 (un) champ non vide si la date de naissance totale ou partielle est connue. Si la date de naissance n'est pas connue, même partiellement, le champ est une chaîne vide «». Les informations devraient correspondre à celles qui figurent sur les documents de voyage. Si des informations sur la date de naissance sont disponibles, l'un des formats ISO 8601 suivants est utilisé. Aucune autre option n'est supportée. YYYY-MM-DD YYYY-MM YYYY (Pour les parties manquantes de la date de naissance, l'application de vérification peut faire appel à la convention XX utilisée dans les documents de voyage lisibles par machine, par exemple 1990-XX-XX.) Exemples: "dob":"1979-04-14" "dob":"1901-08" "dob":"1939" "dob":""

3.3. *Groupes pour les informations spécifiques au type de certificat*

Le schéma JSON supporte trois groupes d'entrées comprenant des informations spécifiques au type de certificat. Chaque EUDCC contient exactement 1 (un) groupe. Les groupes vides ne sont pas autorisés.

Identifiant du groupe	Nom du groupe	Entrées
v	Groupe Vaccination	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (une) dose de vaccin (une dose).
t	Groupe Test	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (un) résultat de test.
r	Groupe Rétablissement	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant 1 (une) déclaration de rétablissement.

▼M1

4. **Informations spécifiques au type de certificat**

4.1. *Certificat de vaccination*

Si le groupe Vaccination est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (un) événement vaccinal (une dose). Tous les éléments du groupe Vaccination sont obligatoires, les valeurs vides ne sont pas supportées.

▼**M1**

Identifiant du champ	Nom du champ	Instructions
v/tg	Maladie ou agent ciblés: COVID-19 (SARS-CoV ou un de ses variants)	Une valeur codée de l'ensemble de valeurs disease-agent-targeted.json. Cet ensemble de valeurs comporte une seule entrée 840539006, qui est le code SNOMED CT (GPS) de la COVID-19. Exactement 1 (un) champ non vide. Exemple: "tg": "840539006"
v/vp	Vaccin ou prophylaxie contre la COVID-19	Type de vaccin ou de prophylaxie utilisé. Une valeur codée de l'ensemble de valeurs vaccine-prophylaxis.json. L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemple: "vp": "1119349007"(un vaccin à ARNm SARS-CoV-2)
v/mp	Produit vaccinal contre la COVID-19	Produit utilisé pour cette dose spécifique de vaccination. ►**M4** Une valeur codée de l'ensemble de valeurs vaccine-medicinal-product.json. Ou une valeur codée renvoyant à un essai clinique et établie suivant la règle figurant au point 3 de l'annexe II. ◄ L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemple: "mp": "EU/1/20/1528" (Comirnaty)
v/ma	Titulaire de l'autorisation de mise sur le marché ou fabricant d'un vaccin contre la COVID-19	Le titulaire de l'autorisation de mise sur le marché ou le fabricant, en l'absence de titulaire d'autorisation de mise sur le marché. ►**M4** Une valeur codée de l'ensemble de valeurs vaccine-mah-manf.json. Ou une valeur codée renvoyant à un essai clinique et établie suivant la règle figurant au point 4 de l'annexe II. ◄ L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemple: "ma": "ORG-100030215"(Biontech Manufacturing GmbH)
v/dn	Nombre dans une série de doses	Le numéro de séquence (entier positif) de la dose administrée au cours de cet événement vaccinal. 1 pour la première dose, 2 pour la deuxième dose, etc. Des règles plus spécifiques figurent à la section 5 de l'annexe II. Exactement 1 (un) champ non vide. Exemples: "dn": "1"(première dose) "dn": "2"(deuxième dose) "dn": "3"(troisième dose)
v/sd	Nombre total de doses dans la série	Le nombre total de doses (entier positif) dans le schéma de vaccination. Des règles plus spécifiques figurent à la section 5 de l'annexe II. Exactement 1 (un) champ non vide. Exemples: "sd": "1"(dans le cas d'un schéma de primovaccination à dose unique) "sd": "2"(dans le cas d'un schéma de primovaccination à deux doses ou d'une dose supplémentaire administrée après un schéma de primovaccination à une dose) "sd": "3"(par exemple, en cas de doses supplémentaires administrées après un schéma de primovaccination à deux doses)

▼M1

Identifiant du champ	Nom du champ	Instructions
v/dt	Date de vaccination	La date d'administration de la dose décrite, au format AAAA-MM-JJ (date complète sans heure). Aucun autre format n'est supporté. Exactement 1 (un) champ non vide. Exemple: "dt": "2021-03-28"
v/co	État membre ou pays tiers dans lequel le vaccin a été administré	Le pays indiqué sous forme d'un code ISO3166 à 2 lettres (RECOMMANDÉ) ou une référence à une organisation internationale responsable de l'événement vaccinal (comme le HCR ou l'OMS). Une valeur codée de l'ensemble de valeurs country-2-codes.json. L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemple: "co": "CZ" "co": "UNHCR"
v/is	Émetteur du certificat	Le nom de l'organisme qui a délivré le certificat. Les identifiants peuvent faire partie du nom, mais il n'est pas recommandé de les utiliser seuls sans le nom sous forme de texte. Maximum 80 caractères en UTF-8. Exactement 1 (un) champ non vide. Exemple: "is": "Ministry of Health of the Czech Republic" "is": "Vaccination Centre South District 3"
v/ci	Identifiant unique du certificat	L'identifiant unique du certificat (UVCI) tel que spécifié à l'adresse https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_ interoperability-guidelines_en.pdf L'inclusion de la somme de contrôle est facultative. Le préfixe "URN:UVCI:" peut être ajouté. Exactement 1 (un) champ non vide. Exemples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Certificat de test*

Si le groupe Test est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (un) résultat de test.

Identifiant du champ	Nom du champ	Instructions
t/tg	Maladie ou agent ciblés: COVID-19 (SARS-CoV ou un de ses variants)	Une valeur codée de l'ensemble de valeurs disease-agent-targeted.json. Cet ensemble de valeurs comporte une seule entrée 840539006, qui est le code SNOMED CT (GPS) de la COVID-19. Exactement 1 (un) champ non vide. Exemple: "tg": "840539006"
t/tt	Type de test	Le type de test utilisé, selon le matériel visé par le test. Une valeur codée de l'ensemble de valeurs test-type.json (sur la base de la nomenclature LOINC). Les valeurs n'appartenant pas à l'ensemble de valeurs ne sont pas autorisées. Exactement 1 (un) champ non vide. Exemple: "tt": "LP6464-4"(Amplification des acides nucléiques avec détection de la sonde) "tt": "LP217198-3"(Immunodosage rapide)

▼M1

Identifiant du champ	Nom du champ	Instructions
t/nm	Nom du test (test d'amplification des acides nucléiques uniquement)	Le nom du test d'amplification des acides nucléiques (TAAN) utilisé. Le nom doit comporter le nom du fabricant du test et la dénomination commerciale du test, séparés par une virgule. Pour les TAAN: ce champ est facultatif. ►M4 Pour les tests de détection d'antigènes: ce champ n'est pas utilisé, car le nom du test est fourni indirectement par l'identifiant du dispositif de test (t/ma). ◄ Lorsqu'il est présent, le champ ne doit pas être vide. Exemple: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"

▼M4

t/ma	Identifiant du dispositif de test (tests de détection d'antigènes uniquement)	Identifiant du dispositif de test de détection d'antigènes provenant de la base de données du JRC. Ensemble de valeurs (liste commune CSS): — Tous les tests de détection d'antigènes figurant sur la liste commune du CSS (lisible par l'homme). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (lisible par machine, les valeurs du champ id_device figurant sur la liste forment l'ensemble de valeurs). Dans les pays de l'UE/EEE, les émetteurs délivrent des certificats uniquement pour les tests appartenant à l'ensemble de valeurs en cours de validité. L'ensemble de valeurs est mis à jour toutes les 24 heures. Les valeurs n'appartenant pas à l'ensemble de valeurs peuvent être utilisées dans les certificats délivrés par des pays tiers, mais les identifiants proviennent toujours de la base de données du JRC. Il n'est pas autorisé d'utiliser d'autres identifiants, tels que ceux fournis directement par les fabricants de tests. Les applications de vérification détectent les valeurs n'appartenant pas à l'ensemble de valeurs actualisé et signalent les certificats comportant ces valeurs comme non valides. Si un identifiant est retiré de l'ensemble de valeurs, les certificats incluant cet identifiant peuvent être acceptés pendant une durée maximale de 72 heures après la date de retrait. L'ensemble de valeurs est distribué à partir du service passerelle DCCUE (*EUDCC Gateway*). Pour les tests de détection d'antigènes: exactement 1 (un) champ non vide. Pour les TAAN: le champ n'est pas utilisé, même si l'identifiant de TAAN est disponible dans la base de données du JRC. Exemple: "ma": "344" (SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)

▼M1

t/sc	Date et heure du prélèvement de l'échantillon	La date et l'heure du prélèvement de l'échantillon. L'heure comprend des informations sur le fuseau horaire. La valeur ne doit pas indiquer l'heure à laquelle le résultat du test a été produit. Exactement 1 (un) champ non vide. L'un des formats ISO 8601 suivants est utilisé. Aucune autre option n'est supportée. YYYY-MM-DDThh:mm:ssZ YYYY-MM-DDThh:mm:ss[+-]hh

▼**M1**

Identifiant du champ	Nom du champ	Instructions
		YYYY-MM-DDThh:mm:ss[+-]hhmm YYYY-MM-DDThh:mm:ss[+-]hh:mm Exemples: "sc": "2021-08-20T10:03:12Z"(UTC) "sc": "2021-08-20T12:03:12+02"(CEST) "sc": "2021-08-20T12:03:12+0200"(CEST) "sc": "2021-08-20T12:03:12+02:00"(CEST)
t/tr	Résultat du test	Le résultat du test. Une valeur codée de l'ensemble de valeurs test-result.json (sur la base de SNOMED CT, GPS). Exactement 1 (un) champ non vide. Exemple: "tr": "260415000"(non détecté)
t/tc	Centre ou installation de test	Nom du centre où le test a été effectué. Les identifiants peuvent faire partie du nom, mais il n'est pas recommandé de les utiliser seuls sans le nom sous forme de texte. Maximum 80 caractères en UTF-8. Tout caractère supplémentaire devrait être tronqué. Le nom n'est pas destiné à faire l'objet d'une vérification automatisée. Pour les tests TAAN exactement 1 (un) champ non vide. ►**M4** Pour les tests de détection d'antigènes: ce champ est facultatif. S'il est présent, il ne doit pas être vide. ◄ Exemple: "tc": "Test centre west region 245"
t/co	État membre ou pays tiers dans lequel le test a été effectué	Le pays indiqué sous forme d'un code ISO3166 à 2 lettres (RECOMMANDÉ) ou une référence à une organisation internationale responsable de l'exécution du test (comme le HCR ou l'OMS). Il s'agit d'une valeur codée de l'ensemble de valeurs country-2-codes.json. L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemples: "co": "CZ" "co": "UNHCR"
t/is	Émetteur du certificat	Le nom de l'organisme qui a délivré le certificat. Les identifiants peuvent faire partie du nom, mais il n'est pas recommandé de les utiliser seuls sans le nom sous forme de texte. Maximum 80 caractères en UTF-8. Exactement 1 (un) champ non vide. Exemples: "is": "Ministry of Health of the Czech Republic" "is": "North-West region health authority"

▼**M1**

Identifiant du champ	Nom du champ	Instructions
t/ci	Identifiant unique du certificat	L'identifiant unique du certificat (UVCI) tel que spécifié à l'adresse vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) L'inclusion de la somme de contrôle est facultative. Le préfixe "URN:UVCI:" peut être ajouté. Exactement 1 (un) champ non vide. Exemples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Certificat de rétablissement*

Si le groupe Rétablissement est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (une) déclaration de rétablissement. Tous les éléments du groupe Rétablissement sont obligatoires, les valeurs vides ne sont pas supportées.

Identifiant du champ	Nom du champ	Instructions
r/tg	Maladie ou agent dont le titulaire s'est rétabli: COVID-19 (SARS-CoV-2 ou un de ses variants)	Une valeur codée de l'ensemble de valeurs disease-agent-targeted.json. Cet ensemble de valeurs comporte une seule entrée 840539006, qui est le code SNOMED CT (GPS) de la COVID-19. Exactement 1 (un) champ non vide. Exemple: "tg": "840539006"
r/fr	Date du premier résultat de ►**M4** ————— ◄ positif du titulaire	La date de prélèvement de l'échantillon pour lequel le ►**M4** ————— ◄ a donné un résultat positif, au format AAAA-MM-JJ (date complète sans heure). Aucun autre format n'est supporté. Exactement 1 (un) champ non vide. Exemple: "fr": "2021-05-18"
r/co	État membre ou pays tiers dans lequel le test a été effectué	Le pays indiqué sous forme d'un code ISO3166 à 2 lettres (RECOMMANDÉ) ou une référence à une organisation internationale responsable de l'exécution du test (comme le HCR ou l'OMS). Il s'agit d'une valeur codée de l'ensemble de valeurs country-2-codes.json. L'ensemble de valeurs est distribué à partir du service passerelle DCCUE *(EUDCC Gateway)*. Exactement 1 (un) champ non vide. Exemples: "co": "CZ" "co": "UNHCR"
r/is	Émetteur du certificat	Le nom de l'organisme qui a délivré le certificat. Les identifiants peuvent faire partie du nom, mais il n'est pas recommandé de les utiliser seuls sans le nom sous forme de texte. Maximum 80 caractères en UTF-8. Exactement 1 (un) champ non vide. Exemple: "is": "Ministry of Health of the Czech Republic" "is": "Central University Hospital"

▼**M1**

Identifiant du champ	Nom du champ	Instructions
r/df	Certificat valide à partir du	La date à partir de laquelle le certificat est considéré comme valide. La date ne doit pas être antérieure à la date calculée selon la formule r/fr + 11 days. La date est indiquée au format AAAA-MM-JJ (date complète sans heure). Aucun autre format n'est supporté. Exactement 1 (un) champ non vide. Exemple: "df": "2021-05-29"
r/du	Certificat valide jusqu'au	Le dernier jour de la période pendant laquelle le certificat est considéré comme valide, fixé par l'émetteur du certificat. Cette date ne doit pas être postérieure à la date calculée selon la formule r/fr + 180 days. La date est indiquée au format AAAA-MM-JJ (date complète sans heure). Aucun autre format n'est supporté. Exactement 1 (un) champ non vide. Exemple: "du": "2021-11-14"
r/ci	Identifiant unique du certificat	L'identifiant unique du certificat (UVCI) tel que spécifié à l'adresse vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) L'inclusion de la somme de contrôle est facultative. Le préfixe "URN:UVCI:" peut être ajouté. Exactement 1 (un) champ non vide. Exemples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

▼M3

ANNEXE VI

RESPONSABILITÉS DES ÉTATS MEMBRES EN QUALITÉ DE RESPONSABLES CONJOINTS DU TRAITEMENT À L'ÉGARD DU SERVICE PASSERELLE POUR LE CERTIFICAT COVID NUMÉRIQUE DE L'UE AUX FINS DE L'ÉCHANGE DE LISTES DE RÉVOCATION D'EUDCC

SECTION 1

Sous-section 1

Répartition des responsabilités

(1) Les responsables conjoints du traitement traitent les données à caractère personnel par l'intermédiaire du service passerelle du cadre de confiance conformément aux spécifications techniques décrites à l'annexe I.

(2) Les autorités de délivrance des États membres demeurent l'unique responsable de la collecte, de l'utilisation, de la divulgation et de tout autre traitement d'informations relatives à la révocation qui ont lieu en dehors du service passerelle, y compris en ce qui concerne la procédure conduisant à la révocation d'un certificat.

(3) Il incombe à chaque responsable du traitement de traiter les données à caractère personnel au sein du service passerelle du cadre de confiance conformément aux articles 5, 24 et 26 du règlement général sur la protection des données.

(4) Chaque responsable du traitement met en place un point de contact doté d'une boîte aux lettres fonctionnelle qui servira à la communication entre les responsables conjoints du traitement, ainsi qu'entre ces derniers et le sous-traitant.

(5) Un groupe de travail institué par le comité visé à l'article 14 du règlement (UE) 2021/953 est mandaté pour trancher toute question relative à l'échange de listes de révocation et à la responsabilité conjointe du traitement de données à caractère personnel correspondant, ainsi que pour faciliter la communication d'instructions coordonnées à la Commission en qualité de sous-traitant. Le processus décisionnel des responsables conjoints du traitement est encadré par ce groupe de travail et régi par le règlement intérieur que ledit groupe doit adopter. À titre de règle de base, la non-participation de l'un des responsables conjoints du traitement à une réunion de ce groupe de travail qui a été annoncée au moins sept (7) jours avant sa convocation par écrit emporte approbation tacite des conclusions de cette réunion du groupe de travail. Tout responsable conjoint du traitement peut convoquer une réunion de ce groupe de travail.

(6) Les instructions à l'intention du sous-traitant sont envoyées par le point de contact de l'un des responsables conjoints du traitement, en accord avec les autres responsables conjoints du traitement, conformément au processus décisionnel du groupe de travail exposé au point 5 ci-dessus. Le responsable conjoint du traitement qui transmet les instructions devrait les communiquer par écrit au sous-traitant et en informer tous les autres responsables conjoints du traitement. Si la question en cause est urgente au point de ne pas permettre la tenue d'une réunion du groupe de travail visé au point (5) ci-dessus, une instruction peut néanmoins être fournie, mais peut être annulée par le groupe de travail. Il conviendrait de communiquer cette instruction par écrit, et tous les autres responsables conjoints du traitement devraient en être informés au moment de sa communication.

(7) The working group as set up per (5) above does not preclude any of the joint controllers' individual competence to inform their competent supervisory authority in accordance with article 33 and 24 of the General Data Protection Regulation. Une telle notification ne nécessite le consentement d'aucun des autres responsables conjoints du traitement.

▼M3

(8) Dans le service passerelle du cadre de confiance, seules les personnes autorisées par les autorités nationales ou les organismes officiels désigné(e)s peuvent avoir accès aux données à caractère personnel échangées.

(9) Chaque autorité de délivrance tient un registre des activités de traitement effectuées sous sa responsabilité. La responsabilité conjointe du traitement peut être indiquée dans le registre.

Sous-section 2

Responsabilités et rôles en matière de traitement des demandes et d'information des personnes concernées

(1) Chaque responsable du traitement, en sa qualité d'autorité de délivrance, fournit aux personnes physiques dont il a révoqué le ou les certificats (les «personnes concernées») des informations sur ladite révocation et sur le traitement de leurs données à caractère personnel dans le service passerelle pour le certificat COVID numérique de l'UE aux fins de permettre l'échange de listes de révocation, conformément à l'article 14 du règlement général sur la protection des données, sauf si la fourniture de ces informations se révèle impossible ou exige des efforts disproportionnés.

(2) Chaque responsable du traitement fait office de point de contact pour les personnes physiques dont il a révoqué le certificat, et traite les demandes présentées par les personnes concernées, ou par leurs représentants respectifs, dans l'exercice de leurs droits conformément au règlement général sur la protection des données. Si un responsable conjoint du traitement reçoit une demande d'une personne concernée qui se rapporte à un certificat délivré par un autre responsable conjoint du traitement, il informe la personne concernée de l'identité et des coordonnées de ce dernier. Sur demande d'un autre responsable conjoint du traitement, les responsables conjoints du traitement se prêtent mutuellement assistance pour le traitement des demandes des personnes concernées et se répondent dans les meilleurs délais, et au plus tard dans un délai d'un mois à compter de la réception d'une demande d'assistance. Si une demande se rapporte à des données communiquées par un pays tiers, le responsable du traitement qui reçoit la demande la traite et informe la personne concernée de l'identité et des coordonnées de l'autorité de délivrance dans le pays tiers.

(3) Chaque responsable du traitement porte à la connaissance des personnes concernées le contenu de la présente annexe, notamment les modalités prévues aux points 1) et 2).

SECTION 2

Gestion des incidents de sécurité, notamment des violations de données à caractère personnel

(1) Les responsables conjoints du traitement se prêtent mutuellement assistance pour la détection et la gestion des incidents de sécurité, notamment des violations de données à caractère personnel, en lien avec le traitement de données dans le service passerelle pour le certificat COVID numérique de l'UE.

(2) En particulier, les responsables conjoints du traitement s'informent mutuellement des éléments suivants:

a) tout risque potentiel ou avéré pour la disponibilité, la confidentialité et/ou l'intégrité des données à caractère personnel faisant l'objet d'un traitement dans le service passerelle du cadre de confiance;

b) toute violation de données à caractère personnel, les conséquences probables de ladite violation et l'évaluation du risque pour les droits et libertés des personnes physiques, ainsi que toute mesure prise pour remédier à la violation de données à caractère personnel et pour atténuer le risque pour les droits et libertés des personnes physiques;

▼**M3**

c) toute atteinte aux garanties techniques et/ou organisationnelles du processus de traitement au sein du service passerelle du cadre de confiance.

(3) Les responsables conjoints du traitement communiquent toute violation de données à caractère personnel relative au processus de traitement au sein du service passerelle du cadre de confiance à la Commission, aux autorités de contrôle compétentes et, lorsqu'ils y sont tenus, aux personnes concernées, conformément aux articles 33 et 34 du règlement général sur la protection des données, ou à la suite d'une notification par la Commission.

(4) Chaque autorité de délivrance met en œuvre des mesures techniques et organisationnelles appropriées, destinées à:

a) garantir et préserver la sécurité, l'intégrité et la confidentialité des données à caractère personnel traitées de manière conjointe;

b) se prémunir contre le traitement, la perte, l'utilisation, la divulgation, l'acquisition non autorisés ou illégaux de toute donnée à caractère personnel en sa possession ou contre l'accès non autorisé ou illégal à ces données;

c) garantir que les données à caractère personnel ne sont ni divulguées ni rendues accessibles à des personnes autres que les destinataires ou les sous-traitants.

SECTION 3

Analyse d'impact relative à la protection des données

(1) Si, afin de s'acquitter des obligations qui lui incombent en application des articles 35 et 36 du règlement (UE) 2016/679, un responsable du traitement a besoin de s'informer auprès d'un autre responsable du traitement, il adresse une demande spécifique à la boîte fonctionnelle visée à la section 1, sous-section 1, point 4). L'autre responsable du traitement met tout en œuvre pour fournir les informations demandées.

▼M3

ANNEXE VII

RESPONSABILITÉS DE LA COMMISSION EN QUALITÉ DE SOUS-TRAITANT DES DONNÉES À L'ÉGARD DU SERVICE PASSERELLE POUR LE CERTIFICAT COVID NUMÉRIQUE DE L'UE EN VUE DE SOUTENIR L'ÉCHANGE DE LISTES DE RÉVOCATION D'EUDCC

La Commission:

(1) met en place et garantit une infrastructure de communication sécurisée et fiable pour le compte des États membres, qui prend en charge l'échange de listes de révocation communiquées au service passerelle pour le certificat COVID numérique.

(2) Afin de s'acquitter de ses obligations en qualité de sous-traitant des données du service passerelle du cadre de confiance pour les États membres, la Commission peut faire appel à des tiers comme sous-traitants ultérieurs; la Commission informe les responsables conjoints du traitement de toute modification envisagée concernant l'ajout ou le remplacement d'autres sous-traitants ultérieurs, donnant ainsi aux responsables du traitement la possibilité de s'opposer conjointement aux modifications de cette nature. La Commission veille à ce que les mêmes obligations en matière de protection des données que celles énoncées dans la présente décision s'appliquent à ces sous-traitants ultérieurs.

(3) La Commission ne traite les données à caractère personnel que sur instruction documentée des responsables du traitement, à moins qu'elle ne soit tenue d'y procéder en application du droit de l'Union ou du droit d'un État membre; dans ce cas, la Commission informe les responsables conjoints du traitement de cette obligation juridique avant de poursuivre l'activité de traitement, sauf si le droit concerné interdit la communication d'une telle information pour des motifs importants d'intérêt public.

Le traitement par la Commission comporte les éléments suivants:

a) l'authentification des serveurs d'arrière-plan nationaux, fondée sur les certificats des serveurs d'arrière-plan nationaux;

b) la réception des données visées à l'article 5 *bis*, paragraphe 3, de la décision téléchargées par les serveurs d'arrière-plan nationaux à l'aide d'une interface de programmation d'application mise à disposition, qui permet aux serveurs d'arrière-plan nationaux de télécharger les données pertinentes;

c) le stockage des données dans le service passerelle pour le certificat COVID numérique de l'UE;

d) la mise à disposition des données aux fins de leur téléchargement par les serveurs d'arrière-plan nationaux;

e) la suppression des données à leur date d'expiration ou sur instruction du responsable du traitement qui les a communiquées;

f) après la fin de la prestation de service, la suppression de toutes les données restantes, à moins que le stockage des données à caractère personnel ne soit exigé au titre du droit de l'Union ou du droit d'un État membre.

(4) La Commission prend toutes les mesures de sécurité à la pointe de la technique nécessaires sur les plans organisationnel, physique et logique pour préserver le service passerelle pour le certificat COVID numérique de l'UE. À cette fin, elle:

a) désigne une entité responsable de la gestion de la sécurité au niveau du service passerelle pour le certificat COVID numérique de l'UE, communique ses coordonnées aux responsables conjoints du traitement et veille à sa disponibilité pour réagir aux menaces pour la sécurité;

▼**M3**

b) est chargée d'assurer la sécurité du service passerelle pour le certificat COVID numérique de l'UE, notamment en procédant régulièrement à des essais, des analyses et des évaluations des mesures de sécurité;

c) veille à ce que toutes les personnes auxquelles est accordé l'accès au service passerelle pour le certificat COVID numérique de l'UE soient soumises à une obligation contractuelle, professionnelle ou légale de confidentialité.

(5) La Commission prend toutes les mesures de sécurité nécessaires pour éviter de compromettre le bon fonctionnement opérationnel des serveurs d'arrière-plan nationaux. À cette fin, elle met en place des procédures particulières relatives à la connexion à partir des serveurs d'arrière-plan au service passerelle pour le certificat COVID numérique de l'UE. Il s'agit notamment:

a) d'une procédure d'évaluation des risques, afin d'identifier et d'estimer les menaces potentielles pour le système;

b) d'une procédure d'audit et de contrôle destinée:

i. à vérifier la correspondance entre les mesures de sécurité mises en œuvre et la politique de sécurité applicable;

ii. à contrôler régulièrement l'intégrité des fichiers système, les paramètres de sécurité et les autorisations accordées;

iii. à assurer une surveillance afin de détecter les atteintes à la sécurité et les intrusions;

iv. à appliquer des modifications afin de corriger les failles existantes en matière de sécurité;

v. à définir les conditions dans lesquelles il convient d'autoriser, notamment à la demande des responsables du traitement, la réalisation d'audits indépendants, y compris des inspections, et d'examens des mesures de sécurité, ainsi que de contribuer à ces opérations, sous réserve de conditions qui respectent le protocole n° 7 du TFUE sur les privilèges et immunités de l'Union européenne;

c) d'une modification de la procédure de contrôle afin de documenter et de mesurer l'incidence des modifications avant leur mise en œuvre et de tenir les responsables conjoints du traitement informés de toute modification susceptible d'affecter la communication avec leurs infrastructures et/ou la sécurité de celles-ci;

d) d'une procédure de maintenance et de réparation afin de préciser les règles et les conditions à respecter lors de la maintenance et/ou de la réparation des équipements;

e) d'une procédure relative aux incidents de sécurité afin de définir le système de signalement et d'escalade, d'informer sans délai les responsables du traitement concernés, d'informer sans délai les responsables du traitement afin qu'ils avertissent les autorités nationales de contrôle de la protection des données, de toute violation de données à caractère personnel et de définir une procédure disciplinaire pour traiter les atteintes à la sécurité.

(6) La Commission prend des mesures de sécurité physiques et/ou logiques à la pointe de la technique pour les installations hébergeant l'équipement du service passerelle pour le certificat COVID numérique de l'UE ainsi que pour les contrôles d'accès de sécurité et les contrôles d'accès aux données logiques. À cette fin, la Commission:

a) assure la sécurité physique, afin de mettre en place des périmètres de sécurité distincts et de permettre la détection des atteintes;

▼M3

b) contrôle l'accès aux installations et tient un registre des visiteurs à des fins de suivi;

c) veille à ce que les personnes extérieures auxquelles l'accès est accordé soient accompagnées par du personnel dûment autorisé;

d) veille à ce que des équipements ne puissent être ajoutés, remplacés ou retirés sans autorisation préalable des organismes compétents désignés;

e) contrôle l'accès au service passerelle du cadre de confiance depuis les serveurs d'arrière-plan nationaux et l'accès depuis ledit service à ces derniers;

f) veille à ce que les personnes qui ont accès au service passerelle pour le certificat COVID numérique de l'UE soient identifiées et authentifiées;

g) réexamine les droits d'autorisation liés à l'accès au service passerelle pour le certificat COVID numérique de l'UE en cas d'atteinte à la sécurité touchant cette infrastructure;

h) préserve l'intégrité des informations transmises par l'intermédiaire du service passerelle pour le certificat COVID numérique de l'UE;

i) met en œuvre des mesures de sécurité d'ordre technique et organisationnel afin d'empêcher l'accès non autorisé aux données à caractère personnel;

j) met en œuvre, en tant que de besoin, des mesures visant à empêcher tout accès non autorisé au service passerelle pour le certificat COVID numérique de l'UE depuis le domaine des autorités de délivrance (c'est-à-dire: blocage d'une localisation/d'une adresse IP).

(7) La Commission prend des mesures pour protéger son domaine, y compris la rupture des connexions, en cas d'écart important par rapport aux principes et concepts de qualité ou de sécurité.

(8) La Commission tient à jour un plan de gestion des risques relatif à son domaine de compétence.

(9) La Commission surveille – en temps réel – la performance de tous les composants de service des prestations au sein du service passerelle du cadre de confiance, produit régulièrement des statistiques et tient des registres.

(10) Pour toutes les prestations du service passerelle du cadre de confiance, la Commission fournit un soutien en anglais, 24 heures sur 24 et 7 jours sur 7, par téléphone, courrier électronique ou portail web, et accepte les appels émanant des appelants autorisés: les coordonnateurs du service passerelle pour le certificat COVID numérique de l'UE et leurs services d'assistance respectifs, les responsables de projets et les personnes désignées de la Commission.

(11) La Commission aide les responsables conjoints du traitement au moyen de mesures techniques et organisationnelles appropriées, dans la mesure du possible, conformément à l'article 12 du règlement (UE) 2018/1725, à s'acquitter de l'obligation qui leur incombe de répondre aux demandes d'exercice des droits de la personne concernée prévus au chapitre III du règlement général sur la protection des données.

▼**M3**

(12) La Commission soutient les responsables conjoints du traitement en fournissant des informations relatives au service passerelle pour le certificat COVID numérique de l'UE, dans le but de mettre en application les obligations énoncées aux articles 32, 33, 34, 35 et 36 du règlement général sur la protection des données.

(13) La Commission veille à ce que les données traitées au sein du service passerelle pour le certificat COVID numérique de l'UE soient incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès.

(14) La Commission prend toutes les mesures appropriées pour empêcher que les opérateurs du service passerelle pour le certificat COVID numérique de l'UE disposent d'un accès non autorisé aux données transmises.

(15) La Commission prend des mesures pour faciliter l'interopérabilité et la communication entre les responsables du traitement désignés du service passerelle pour le certificat COVID numérique de l'UE.

(16) La Commission tient, conformément à l'article 31, paragraphe 2, du règlement (UE) 2018/1725, un registre des activités de traitement effectuées pour le compte des responsables conjoints du traitement.