sesam-vitale

Appli carte Vitale

*Référentiel d'exigences minimales*

# APPLI CARTE VITALE REFERENTIEL D'AUTORISATION DE L'UTILISATION DE L'APPLICATION CARTE VITALE (« APPLI CARTE VITALE ») POUR AUTHENTIFIER A DISTANCE LES UTILISATEURS

Statut : Validé
Version : 1.2
Diffusion : publique

**GIE SESAM-Vitale**
5, boulevard Marie et Alexandre Oyon – 72019 LE MANS CEDEX 2
www.sesam-vitale.fr

Ce document a été élaboré par le GIE SESAM-Vitale.

# TABLE DES MATIERES

# 1 OBJET ET DESTINATAIRES DU REFERENTIEL

Le référentiel d'autorisation de l'appli carte Vitale décrit les exigences à respecter et apporte des préconisations pour un Fournisseur de Services souhaitant implémenter l'authentification à distance de l'utilisateur de *l'appli carte Vitale*.

Dans ce référentiel des documents et standards à respecter sont mentionnés.

Les Fournisseurs de Services souhaitant implémenter l'authentification à distance de l'utilisateur de *l'appli carte Vitale* doivent s'appuyer sur la dernière version publiée du référentiel.

Il est à noter que la numérotation des exigences est faite de manière à garantir l'absence de renumérotation. Ainsi, en cas de publication d'une nouvelle version du référentiel et de l'ajout de nouvelles exigences, ces dernières seront numérotées de manière incrémentale par rapport aux exigences préexistantes

# 2 APPLI CARTE VITALE

## 2.1 Qu'est-ce que l'appli carte Vitale ?

L'appli carte Vitale est une solution numérique développée par le GIE SESAM-Vitale pour le compte des organismes d'assurance maladie obligatoire. Elle constitue une alternative numérique à la carte Vitale physique sous la forme d'une application pour smartphone, disponible sous Android et iOS, facile d'accès et simple d'utilisation. Il s'agit de proposer aux assurés une solution dématérialisée et sécurisée d'identification et d'authentification numérique.

L'application bénéficie d'une sécurité renforcée grâce à une double authentification, garantissant que seul l'utilisateur autorisé peut y accéder. Elle permet d'assurer l'identification électronique de ses détenteurs sur des services accessibles sur internet.

C'est ce cas d'usage de fournisseur d'identité des utilisateurs ayant activé leur appli carte Vitale qui fait l'objet de ce référentiel.

## 2.2 Qu'est-ce qu'un fournisseur d'identité ?

Le Fournisseur d'identité appli carte Vitale est un service qui authentifie les utilisateurs grâce à leur appli carte Vitale et délivre des jetons conformes au standard OpenId Connect pour sécuriser l'accès au service numérique du Fournisseur de Services.

## 2.3 Qu'est-ce qu'un fournisseur de Services ?

Le Fournisseur de Services désigne toute personne morale immatriculée dans l'Union européenne, fournissant un service numérique à des utilisateurs, et autorisé à utiliser l'appli carte Vitale conformément à la Convention d'autorisation de l'appli carte Vitale.

# 3 DOCUMENTATIONS ET LIENS UTILES

| DOCUMENTATION | LIENS UTILES |
|---|---|
| Documentation juridique | Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juin 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit « règlement eIDAS » et ses actes d'exécution publiés sur le site de l'ANSSI : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/<br><br>Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit « règlement RGPD » : RÈGLEMENT (UE) 2016/ 679 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 27 avril 2016 - relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/ 46/ CE (règlement général sur la protection des données)<br><br>Article L. 1470-3 du code de la santé publique : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043497483?init=true&page=1&query=Article+L.1470-3+&searchField=ALL&tab_selection=all<br><br>Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « LIL » https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460?init=true&page=1&query=Loi+n%C2%B0+78-17+du+6+janvier+1978+relative+%C3%A0+l%27informatique%2C+aux+fichiers+et+aux+libert%C3%A9s&searchField=ALL&tab_selection=all<br><br>Article R-161-33-15 du code de la sécurité sociale |
| Référentiel de la PGSSI-S sur l'identification électronique | https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication |
| OpenId Connect | https://openid.net/connect/ |
| Implémentations OpenId Connect | https://openid.net/developers/certified/ |
| Guide d'implémentation de l'INS | https://esante.gouv.fr/produits-services/referentiel-ins |
| Guide d'intégration Authentifier à distance l'utilisateur d'une appli carte Vitale | Espace industriels du GIE SESAM-Vitale (https://industriels.sesam-vitale.fr) |

# 4 REFERENTIEL APPLI CARTE VITALE

| | |
|---|---|
| EX-APCV-XX | L'ensemble des exigences sont identifiables par un encadré gris |

| | |
|---|---|
| RC-APCV-XX | L'ensemble des recommandations sont identifiables par un encadré blanc |

## 4.1 Portée des exigences et recommandations du référentiel

Les exigences et recommandations ci-après, définies par le GIE SESAM-Vitale, sont à respecter par les différents acteurs visés dans le présent référentiel.

Le GIE SESAM-Vitale pourra étudier à titre d'exception la levée de certaines de ces exigences dans le cadre de demandes et de situations justifiées.

## 4.2 Éligibilité à l'appli carte Vitale et procédure d'autorisation

Pour intégrer l'appli carte Vitale, les Fournisseurs de Services doivent satisfaire plusieurs prérequis, détaillés ci-après.

| **EX-APCV-01 : Identification électronique pour les fonctionnalités liées à l'appli carte Vitale** |
|---|
| Le Fournisseur de Services DOIT proposer à ses utilisateurs des fonctionnalités qui nécessitent leur identification électronique pour les cas d'usage ouverts (liste sur le site du GIE SESAM-Vitale). |

| **EX-APCV-02 : RGPD et Loi Informatique et Libertés** |
|---|
| Le Fournisseur de Services DOIT respecter la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le Règlement général sur la protection des données (RGPD) |

## 4.3 Modalités de raccordement technique

| **RC-APCV-01 : Utilisation d'implémentations OpenId Connect certifiées** |
|---|
| Le Fournisseur de Services DEVRAIT utiliser une implémentation OpenId Connect issue d'une librairie certifiée par la fondation OpenId Connect, plutôt que de développer une solution spécifique. La liste des implémentations certifiées est accessible sur le site officiel de la fondation. |

| **EX-APCV-03 : Utilisation d'OpenId Connect** |
|---|
| Le Fournisseur de Services DOIT utiliser les flux OpenId Connect définis par le Fournisseur d'identité appli carte Vitale. |

| **EX-APCV-04 : Suppression des contextes OIDC** |
|---|
| Le Fournisseur de Services DOIT réinitialiser et supprimer tous les contextes OpenId Connect de l'utilisateur et toutes les informations de session associées conservées localement lorsque l'utilisateur se déconnecte de son service. |

| **EX-APCV-05 : Protection des secrets du Fournisseur de Services** |
| --- |
| Le Fournisseur de Services DOIT s'assurer que les informations de raccordement[1] persistantes nécessaires à l'authentification ne sont pas présentes dans le code source, qu'elles sont stockées de façon sécurisée et qu'elles ne sont jamais conservées au-delà de leur durée de validité. |

## 4.4 Environnement de test

| **EX-APCV-06 : Accessibilité du service de test** |
| --- |
| Le Fournisseur de Services DOIT donner accès au GIE SESAM-Vitale à son service de test lorsque le GIE SESAM-Vitale le demande. |

| **EX-APCV-07 : Jeux de données de test** |
| --- |
| Le Fournisseur de Services DOIT uniquement utiliser des jeux de données de test, par opposition à des données réelles, dans le cadre de ses travaux sur un environnement de tests. Aucune donnée réelle ne doit figurer dans les jeux de test. |

## 4.5 Blocage des mésusages

| **EX-APCV-08 : Blocage des utilisateurs malveillants** |
| --- |
| Le Fournisseur de Services DOIT mettre en place un processus permettant de bloquer les utilisateurs malveillants. |

## 4.6 Gestion et fusion des comptes avec d'autres moyens d'identification électronique

Lorsque le Fournisseur de Services dispose de moyens d'identification électronique préexistants et/ou complémentaires à l'appli carte Vitale, il les maintient s'ils sont conformes au référentiel d'identification électronique de la PGSSI-S.

| **EX-APCV-09 : Fusion de comptes** |
| --- |
| Le Fournisseur de Services DOIT permettre à l'utilisateur de fusionner ses identités créées avec différentes modalités d'authentification en un compte unique, via une procédure permettant de garantir que l'utilisateur a demandé la fusion et qui garantit également la sécurité (intégrité, confidentialité) et la cohérence des données fusionnées ainsi que la traçabilité de la fusion. Cette procédure doit nécessiter l'authentification par l'appli carte Vitale. Si le Fournisseur de Services dispose de l'Identité Nationale de Santé (INS) de l'utilisateur de l'appli carte Vitale, le Fournisseur de Services DOIT vérifier la correspondance entre les INS avant de proposer de fusionner les identités.<br><br>Sinon, la réconciliation doit être basée a minima sur les 5 traits d'identité (Nom de naissance, 1er prénom de naissance (simple ou composé), sexe, date de naissance, lieu de naissance).<br><br>cf. Modalités définies dans le Guide d'implémentation de l'INS. |

[1] On appelle *informations de raccordement* les éléments nécessaires à l'authentification du service auprès du fournisseur d'identité appli carte Vitale, par exemple le client Id et le client secret, ou les clefs privées des certificats X509 d'authentification.

## 4.7 Sécurité

### 4.7.1 Sécurité opérationnelle

Les paramètres de sécurité de la protection des flux entre le Fournisseur de Services et le Fournisseur d'identité de l'appli carte Vitale respectent les préconisations de l'ANSSI.

Dans ce référentiel, un « client lourd » désigne une application native fournie par un Fournisseur de Services, fonctionnant indépendamment du navigateur internet installé sur l'appareil de l'utilisateur. Il peut s'agir, par exemple, d'applications installées localement sur des postes de travail ou de logiciels mobiles déployés via les magasins d'applications des systèmes d'exploitation.

Dans le cadre de l'OpenId Connect, le client lourd joue un rôle spécifique en tant qu'interface proposée par le Fournisseur de Services pour accéder aux fonctionnalités qu'il offre. Cependant, pour la gestion des cinématiques OpenId Connect (telles que le « Authorization Code Flow »), ces clients doivent s'appuyer sur un navigateur web.

Hors l'intégration d'un composant de navigation web interne tel que les « webviews » dans une application client lourd, les cas suivants soulèvent des problématiques de sécurité, notamment :

- l'absence de visibilité sur la maintenance des noyaux logiciels des composants intégrés ;
- la difficulté de déployer rapidement une mise à jour de sécurité sur l'ensemble du parc des clients lourds concernés en cas de vulnérabilité détectée ;
- le risque qu'un client lourd non maintenu ou non mis à jour reste opérationnel, augmentant l'exposition aux risques de sécurité.

En revanche, l'utilisation de navigateurs web externes grand public est privilégiée pour les raisons suivantes :

- une visibilité accrue sur la maintenance grâce à des publications officielles et publiques ;
- des mises à jour automatiques configurées par défaut sur la majorité des appareils ;
- une politique d'obsolescence des versions anciennes, documentée et appliquée par les éditeurs

Une tolérance peut être envisagée pour les applications hybrides intégrant un composant de navigation web respectant les standards de sécurité et de maintenance des navigateurs grand public.

| **EX-APCV-10 : Utilisation d'un navigateur web externe pour les flux OpenId Connect** |
|---|
| Le Fournisseur de Services disposant d'un client lourd sur poste de travail DOIT s'appuyer sur un navigateur externe à son application pour exécuter la cinématique "Authorization Code Flow" définie dans le cadre de l'OpenId Connect du Fournisseur d'Identité appli carte Vitale. |

Le GIE SESAM-Vitale se réserve le droit de faire évoluer les modalités techniques du Fournisseur d'identité appli carte Vitale, notamment en matière de sécurité pour tenir compte des préconisations de la PGSSI-S[2].

| **EX-APCV-11 : Conformité** |
|---|
| Le Fournisseur de Services DOIT respecter les préconisations sécuritaires du service de l'appli carte Vitale notifiées par le GIE SESAM-Vitale auprès du responsable technique du Fournisseur de Services. |

[2] https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication

Le GIE SESAM-Vitale communiquera directement auprès des contacts fournis lors du raccordement, les informations utiles en cas de modifications critiques de ces préconisations. Par ailleurs, en cas d'incident de sécurité sur son service, en particulier si cet incident a un lien avec l'appli carte Vitale, le Fournisseur de Services doit le signaler au GIE SESAM-Vitale.

| **EX-APCV-12 : Notification des incidents de sécurité et des violations de données** |
|---|
| En cas de suspicion forte ou de détection avérée d'un incident de sécurité, en cas d'attaques cybercriminelles ou d'une violation de données à caractère personnel, impactant directement ou indirectement l'appli carte Vitale, son usage ou ses données, le Fournisseur de Services DOIT prévenir le GIE SESAM-Vitale immédiatement après la détection et au plus tard dans les 72h, même si les détails complets de l'incident ne sont pas encore disponibles.<br><br>On entend par suspicion forte de violation de données, toute suspicion basée sur des éléments objectifs permettant de conclure à une probabilité forte que la violation de données soit avérée. |

| **EX-APCV-13 : Veille sécuritaire** |
|---|
| Le Fournisseur de Services DOIT mener sur son périmètre une veille cybersécurité, incluant la surveillance continue des vulnérabilités connues affectant les composants logiciels (y compris bibliothèques et frameworks utilisés), matériels et infrastructures utilisés dans les services en lien avec l'appli carte Vitale, afin d'identifier rapidement toute faille de sécurité, mise à jour critique ou fin de support pouvant impacter la sécurité desdits services. |

| **EX-APCV-14 : Traçabilité des accès et conservation des données afférentes** |
|---|
| Le Fournisseur de Services DOIT mettre en œuvre les mesures nécessaires pour assurer la traçabilité des accès à son service avec l'appli carte Vitale. Il est responsable de la conservation de ces informations à des fins probatoires ou pour tout autre besoin justifié. |

### 4.7.2 Sécurité du système d'information

| **EX-APCV-15 : Gouvernance relative à la sécurité des systèmes d'information** |
|---|
| Le Fournisseur de Services DOIT mettre en place une organisation relative à la sécurité des systèmes d'information et disposer d'une politique de sécurité des systèmes d'information (PSSI). |

| **EX-APCV-16 : Actions de sensibilisation des équipes aux mesures de sécurité** |
|---|
| Le Fournisseur de Services DOIT mettre en place des actions de sensibilisation aux règles et bonnes pratiques de manipulation des données pour l'ensemble de ses équipes ainsi que des actions de formation pour les équipes chargées de la sécurité des systèmes d'information. |

| **EX-APCV-17 : Évaluation et maitrise des risques** |
|---|
| Le Fournisseur de Services DOIT mettre en place un processus d'évaluation des risques[3] sur son système d'information en lien avec l'usage de l'appli carte Vitale en matière de sécurité des systèmes d'information. Il définit et applique un plan destiné à maintenir à niveau la sécurité, notamment lors des évolutions du système d'information. |

[3] Il peut aussi bien s'agir d'une analyse de risques réalisée sur une norme établie conforme ISO 27005/2022 (ex : EBIOS RM) que d'une analyse de risques ad hoc.

| **EX-APCV-18 : Contrôle des flux réseau et applicatifs** |
|---|
| Le Fournisseur de Services DOIT mettre en place un ou plusieurs mécanismes de protection réseau et applicatifs incluant une rupture protocolaire de niveau 7 en entrée du service (WAF, reverse proxy, XML gateway, IDS/IPS, anti-DDoS, firewall, etc.). Ceux-ci DOIVENT être paramétrés pour prévenir les principaux types d'attaque (telles que les attaques par déni de service ou par force brute ainsi que les types d'attaques décrits dans le Top 10 OWASP) à adapter en fonction des risques identifiés dans le cadre de l'analyse de risques. |

| **RC-APCV-02 : Développement sécurisé** |
|---|
| Le Fournisseur de Services DEVRAIT s'assurer que ses développements réalisés respectent les guides de bonnes pratiques en matière de développements sécurisés, notamment ceux édités par l'ANSSI et la CNIL. |

| **EX-APCV-19 : Gestion des accès** |
|---|
| Le Fournisseur de Services DOIT mettre en place une politique de gestion des privilèges d'accès logique et physique conforme aux bonnes pratiques de sécurité, se traduisant notamment par l'attribution des habilitations selon le principe de moindre privilège et du besoin d'en connaitre.<br><br>Le Fournisseur de Services opère une revue annuelle des comptes d'accès aux ressources informatiques (serveurs, postes de travail, applications). |

| **EX-APCV-20 : Audits** |
|---|
| Le Fournisseur de Services DOIT mener des audits[4] techniques (audit de code, tests d'intrusion…) et organisationnels afin d'identifier et corriger d'éventuelles vulnérabilités. Les audits doivent donner lieu à l'élaboration d'un plan d'action. Un audit doit être pratiqué avant l'ouverture du service, puis régulièrement tous les 3 ans, a minima. |

## 4.8 Identité visuelle

L'appli carte Vitale peut être proposée à côté d'autres moyens d'identification. Dans ce cas, il est obligatoire d'intégrer les boutons de l'appli carte Vitale au même niveau que les autres méthodes de connexions proposées par le service : dans une même zone graphique, tous les moyens d'identification électronique doivent être visibles et mis sur un pied d'égalité.

| **EX-APCV-21 : Intégration de l'identification électronique par l'appli carte Vitale** |
|---|
| Le Fournisseur de Services DOIT intégrer l'identification électronique par l'appli carte Vitale au moins au même niveau que les autres modalités d'identification électronique proposées aux utilisateurs. |

| **EX-APCV-22 : Graphisme du bouton** |
|---|
| Le Fournisseur de Services DOIT utiliser l'un des éléments graphiques de type boutons fournis par le GIE SESAM-Vitale pour l'intégration de l'appli carte Vitale conformément à la charte graphique définie et disponible sur l'espace industriels du GIE SESAM-Vitale (https://industriels.sesam-vitale.fr). |

| **EX-APCV-23 : L'essentiel sur l'appli carte Vitale** |
|---|
| Le Fournisseur de Services DOIT afficher le lien vers le site appli carte Vitale « Qu'est-ce que l'appli carte Vitale ». |

[4] Les audits peuvent être réalisés en interne si le Fournisseur de Services dispose de ressources avec l'expertise sécurité requise (auditeurs expérimentés) ou faire l'objet d'une prestation externe, qualifiée ou non, par un prestataire reconnu sur le marché.

## 4.9 Éthique

| **EX-APCV-24 : Simple et intuitive** |
|---|
| Le Fournisseur de Services DOIT intégrer l'appli carte Vitale comme moyen d'identification électronique à son service en garantissant une expérience d'accès simple et intuitive pour les utilisateurs. |

| **EX-APCV-25 : Compréhensible** |
|---|
| Le Fournisseur de Services DOIT mettre en œuvre des mécanismes permettant de garantir la bonne compréhension de l'usage de l'appli carte Vitale par l'utilisateur du service. |

| **RC-APCV-03 : Assistance** |
|---|
| Le Fournisseur de Services DEVRAIT mettre à disposition de l'utilisateur un service d'assistance pour faciliter sa compréhension des utilisations de l'appli carte Vitale comme moyen d'identification électronique. |

| **RC-APCV-04 : Accessibilité** |
|---|
| Le Fournisseur de Services DEVRAIT garantir un niveau de conformité suffisant au RGAA (Référentiel Général d'Amélioration de l'Accessibilité) et réaliser des audits réguliers, tester ses services et mettre en place un plan de correction des non-conformités. |

| **EX-APCV-26 : Accessibilité pour les services soumis RGAA** |
|---|
| Si ses services sont soumis au RGAA, le Fournisseur de Services DOIT garantir un niveau de conformité suffisant au RGAA (Référentiel Général d'Amélioration de l'Accessibilité) et réaliser des audits réguliers, tester ses services et mettre en place un plan de correction des non-conformités. |

| **EX-APCV-27 : Développement durable** |
|---|
| Le Fournisseur de Services utilisant l'appli carte Vitale DOIT être engagé en matière de développement durable, en mettant en œuvre des mesures visant à réduire son empreinte écologique[5], à garantir l'accessibilité numérique pour tous, et à adopter des pratiques socialement responsables et économiquement viables. |

[5] Des processus sont mis en œuvre par le fournisseur du service afin de réduire l'impact environnemental du recours à l'appli carte Vitale. Il conduit, par exemple, des actions de réduction des émissions de gaz à effet de serre et d'adaptation au changement climatique.

# 5 GLOSSAIRE

| | |
|---|---|
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| CNIL | Commission Nationale de l'Informatique et des Libertés |
| OIDC | OpenId Connect |
| FI | Fournisseur d'identité |
| FS | Fournisseur de Services |
| INS | Identité Nationale de Santé |
| PGSSI-S | Politique Générale de Sécurité des Systèmes d'Information de Santé |
| PSSI | Politique de Sécurité des Systèmes d'Information |
| RGAA | Référentiel Général d'Amélioration de l'Accessibilité |
| RGPD | Règlement général sur la protection des données |