AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Introduction à l'Espace de Confiance DRIM-M (mesimagesmedicales.fr)

Mes Images Médicales

Version externe

Statut : Validé | *Classification : Publique* | *Version : 1.1*

Agence du Numérique en Santé
2 – 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Destinataires

Les destinataires de ce document sont principalement les Opérateurs de DRIMbox et leurs Clients qui souhaitent intégrer l'Espace de Confiance DRIM-M en déployant et maintenant une DRIMbox conformément aux Conditions Générales d'Intégration à l'Espace de Confiance DRIM-M (CGI) et au parcours décrit dans le Guide d'Intégration à l'Espace de Confiance DRIM-M.

Historique du document

Version	Date de publication	Motif et nature de la modification
1.0	29 juillet 2025	Création du document
1.1	17 septembre 2025	Amendement du document

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Définitions

Les termes définis ci-après, qu'ils apparaissent au singulier ou au pluriel dans le présent document, auront la signification suivante lorsqu'ils commencent par une majuscule :

Autorité de certification : désigne un tiers de confiance du marché qui délivre des certificats et met à disposition des moyens de vérification de validité des certificats qu'elle a fournis.

Bureau d'enregistrement : désigne un prestataire reconnu pour leur expertise dans l'enregistrement et la gestion des noms de domaine. Il agit en intermédiaire entre le titulaire du domaine et le registre officiel qui détient les bases de données de nom de domaine.

Certificat SSL : désigne un fichier numérique qui permet d'identifier et chiffrer les communications entre un site web et ses utilisateurs.

Client : désigne les centres d'imagerie ou les établissements de santé ayant une activité déclarée de radiologie et/ou de médecine nucléaire et bénéficiaires d'une instance du logiciel DRIMbox.

CSR (Certificate Signing Request): désigne une demande de signature de certificat. Il s'agit d'un texte chiffré généré par le propriétaire du site web, contenant sa clé publique et des informations d'identification. Cette CSR est envoyée à l'autorité de certification pour obtenir un certificat SSL.

DCV (Domain Control Validation) : désigne la validation du contrôle de domaine. Le challenge DCV consiste à prouver la propriété du nom de domaine pour le demandeur du certificat SSL. Il se fait via trois méthodes : ajout d'enregistrement DNS, fichier/http ou email.

DNS (Domain Name Server) : désigne un système qui associe les noms de domaine aux adresses IP correspondantes aux serveurs. Il joue un rôle fondamental dans l'acheminement des requêtes Internet.

DMP (Dossier Médical Partagé) : désigne un service socle de la CNAM qui permet d'accéder au dossier du patient (traitement, antécédents, allergies...). Il permet également le partage sécurisé de l'information entre professionnels de santé.

DRIMbox : désigne une passerelle intégrée ou interfacée au système d'information des Clients qui connecte leur(s) PACS au maillage DRIM-M. L'ensemble des DRIMbox intégrées à l'Espace de Confiance forme le maillage DRIM-M. L'Espace de Confiance vise à sécuriser le maillage DRIM-M.

DRIM-M (Data Radiologie Imagerie Médicale & Médecine Nucléaire) : désigne le projet porté par le programme « le Ségur du numérique en santé » avec l'objectif de créer un réseau unique national de partage d'images à destination des professionnels de santé et des patients

DRIMbox consommatrice : désigne une des 2 fonctions de la DRIMbox. La DRIMbox se connecte au DMP en consultation, elle récupère un à plusieurs pointeurs (ou *Manifest KOS*) correspondant à un patient identifié et qualifié. A l'aide des identifiants contenus dans les pointeurs récupérés, elle télécharge les images auprès de la DRIMbox fonction Source qui elle-même est reliée au PACS. Elle peut ensuite soit :

- Proposer directement une visualisation de ces examens d'imagerie grâce à une Visionneuse DICOM non-diagnostic minimum présent sur la DRIMbox fonction Conso ;
- Exporter les examens récupérés pour qu'ils soient enregistrés dans le PACS ou tout autre système consommateur compatible avec le standard DICOM.

DRIMbox mutualisée : désigne un service de partage d'imagerie médicale mutualisé entre différents établissements de soins. Plusieurs RIS et plusieurs PACS provenant de ces différentes structures peuvent alors être reliés à une instance DRIMbox.

DRIMbox source : désigne une des 2 fonctions de la DRIMbox. L'émission du compte-rendu d'imagerie validé vers le DMP depuis le logiciel RIS (Système d'information radiologique) déclenche en parallèle l'émission d'une copie du compte-rendu d'imagerie depuis le RIS vers la DRIMbox fonction Source. Avec les informations présentes dans le

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

compte-rendu d'imagerie mais aussi dans le message le transportant, la DRIMbox construit un pointeur de Références d'objets d'un Examen d'Imagerie (*Manifest KOS*) grâce à la requête du PACS (*Picture Archiving and Communication System*) relié à la DRIMbox sur lequel les images sont stockées, ce pointeur est ensuite envoyé au DMP. La DRIMbox fonction Source expose également une Visionneuse DICOM non-diagnostic minimum pour permettre l'affichage des examens à partir de liens présents sur les comptes-rendus d'imagerie, ces liens sont positionnés par le RIS au moment de la rédaction et validation des comptes-rendus d'imagerie.

Editeur : désigne toute personne physique ou morale, publique ou privée, ou tout groupement de personnes, doté ou non de la personnalité morale, qui édite la Solution logicielle, candidate au référencement par l'Agence du Numérique en Santé.

Espace de Confiance : désigne
- Un **Registre National d'identification** dont le rôle est d'assigner des noms de domaines uniques, pérennes et de confiance, gérés et distribués par l'ANS à chaque DRIMbox déployée
- Un **Domaine déposé par l'ANS** et utilisé dans le maillage DRIM-M (mesimagesmedicales.fr)
- Une **Liste Blanche** signée par l'ANS et répertoriant les DRIMbox de confiance
- Une **Météo des DRIMbox** qui permettra d'informer l'écosystème du statut opérationnel des DRIMbox

FQDN (Fully Qualified Domain Name) : désigne un nom de domaine complet, unique, pérenne, de confiance, géré et distribué par l'ANS à chaque DRIMbox déployée. (Exemple : db1.1.mesimagesmedicales.fr)

Introspection : désigne la possibilité pour un fournisseur de service (FS) de valider un jeton auprès du serveur d'authentification (AS)d'authentification de Pro Santé Connect (PSC).

KOS (ou Manifest KOS) : désigne un document normalisé par le standard DICOM, contenant un pointeur référençant un examen d'imagerie médicale d'un patient. Le KOS référence l'ensemble des identifiants que comporte un examen d'imagerie.

Liste Blanche : désigne un fichier XML signé par l'ANS avec un certificat de l'offre ORG SIGN émis par l'IGC Santé, contenant la liste des DRIMbox opérationnelles intégrées au sein de l'Espace de Confiance. Elle est gérée par l'ANS qui est charge de

- La validation des demandes de mise à jour du fichier initiées par les Opérateurs concernant les ajouts, retraits et modifications des DRIMbox ;
- Du retrait des DRIMbox de la Liste Blanche dans le respect des règles d'exclusion et réintégration.

Météo des Services DRIMbox : désigne une page de statut publique qui informe de la disponibilité des DRIMbox de l'Espace de Confiance et ses PACS associés en temps réel, disponible à travers le lien suivant : https://status.drimm.esante.gouv.fr.

Opérateur : désigne la personne morale réalisant pour le compte du Client le déploiement, l'intégration au sein de l'Espace de Confiance et le maintien en condition opérationnelle d'une ou plusieurs DRIMbox. L'Opérateur peut être l'Editeur ou le Distributeur.

PACS (Picture Archiving and Communication System) : désigne un système d'information permettant un archivage et une diffusion des images réalisées dans les services de radiologie et médecine nucléaire.

ProSanté Connect : désigne le Fournisseur d'Identité (FI) de la santé. C'est un service standard (protocole OpenID) et gratuit, développé et maintenu par l'ANS.

Proxy e-santé : désigne tout service de type proxy ayant adhéré au niveau Pro Santé Connect – Extension Espace de Confiance. Ce serveur intermédiaire, ne disposant pas d'interface utilisateur, est destiné à sécuriser les échanges de données au sein de l'Espace de Confiance PSC, ayant permis l'authentification de l'utilisateur par PSC et l'API Pro Santé Connectée.

Registre national d'identification des DRIMbox : désigne un fichier qui regroupe l'ensemble des informations relatives aux DRIMbox Sources déployées (identification des Opérateurs et leur contacts, 2 FQDN uniques à minima (DRIMbox et visionneuse) attribués par l'ANS). Il est hébergé et maintenu par l'ANS. Si le Client possède n PACS à relier à la DRIMbox, l'ANS attribuera n groupes de 2 FQDN.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

RIS (Radiology Information System) : désigne le logiciel métier du radiologue ou médecin nucléaire leur permettant d'accèder à de nombreuses fonctionnalités telles que la prise de rendez-vous, la création et la gestion des comptes-rendus, la facturation etc.

Site : désigne un emplacement géographique sur lequel une à plusieurs DRIMbox sont déployées par un Opérateur pour une commande. Cette information est définie par la liste du SIREN des structures clientes concernées.

URL (Uniform Resource Locator) (=Fully Qualified Domain Name) : désigne une adresse complète qui identifie une ressource web. Une URL indique à la fois le protocole, nom de domaine et chemin d'accès.

Acronymes

DCV	Domain Control Validation
DNS	Domain Name Server
DMP	Dossier Médical Partagé
KOS	Key Object Selection
CR	Compte-Rendu
CSR	Certificate Signing Request
PACS	Picture Archiving and Communication System
RIS	Radiology Information System
DB	DRIMbox
DRIM-M	Data Radiologie Imagerie Médicale & Médecine Nucléaire
ANS	Agence du Numérique en Santé
DICOM	Digital Imaging and Communications in Medicine
PS	Professionnel de Santé
LPS	Logiciel des Professionnels de Santé
URL (FQDN)	Uniform Resource Locator (=Full Qualified Domain Name)

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

SOMMAIRE

1. LE CONTEXTE 6
1.1. Le projet DRIM-M 6
Son objectif 6
Les bénéfices attendus 6
La DRIMbox 6
Ses deux usages de consommation des images 6
1.2. Introduction à l'Espace de Confiance DRIM-M 7
Un compromis en matière de sécurité pour ne pas freiner l'usage métier 7
Ses objectifs 7
Ses acteurs 7
2. L'ESPACE DE CONFIANCE 8
2.1. Le Registre National 8
Les origines de la création du Registre National 8
2.2. Le nom de domaine 8
La présentation de la structure des URL 8
La gestion du DNS et bureau d'enregistrement 9
Les règles d'attribution des FQDN en fonction des architectures 9
2.3. La Liste Blanche 10
La Liste Blanche 10
Sa signature et sa publication 11
2.4. La météo des services 12
2.5 Les certificats 12
Le besoin en certificat IGC-Santé 12
Le besoin en certificat du marché 13
2.5. La validation du contrôle de domaine 15
2.6 L'automatisation de la gestion des certificats 15
L'automatisation de la gestion des certificats IGC-Santé 15
L'automatisation de la gestion des certificats du marché 16

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

1. LE CONTEXTE

1.1. Le projet DRIM-M

Le projet DRIM-M (Data Radiologie Imagerie Médicale & Médecine Nucléaire) résulte d'un **programme** le Ségur du numérique en santé, d'un **besoin** de partage en imagerie médicale au niveau national et d'un **partenariat** entre radiologues et pouvoirs publics.

Son objectif

Son objectif est la création d'un **réseau unique et national de partage d'images** à destination des professionnels de santé et des patients : le **maillage DRIM-M.**

Les bénéfices attendus

- Les images restent là où elles sont produites (dans les PACS des structures sources). Ainsi, le réseau facilite le partage de manière sécurisée et décentralisée.
- Le projet DRIM-M permet entres autres, d'éviter la duplication des demandes d'examens d'imagerie médicale.
- Il offre également une vue complète de l'historique médical afin d'améliorer la continuité et qualité de la prise en charge.

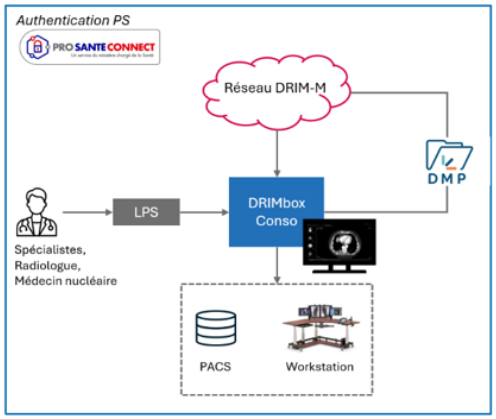
La DRIMbox

Chaque service et cabinet de radiologie/médecin nucléaire est un nœud du maillage DRIM-M à travers sa passerelle DRIMbox dont il connecte son PACS et RIS.

Ses deux usages de consommation des images

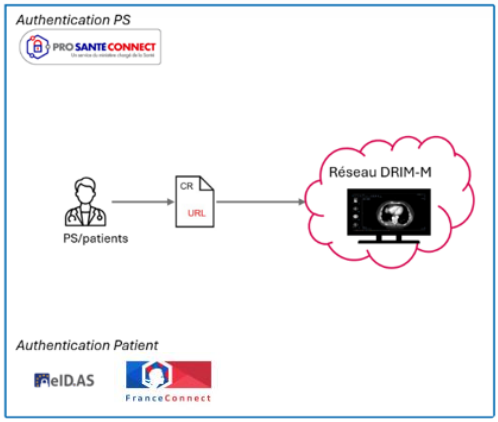
Pour les PS exploitants de l'imagerie: radiologues et médecins nucléaires (et tous PS habilités)

Visualiser **et/ou** importer un ou plusieurs examens dans son environnement d'imagerie afin de réaliser des **comparaisons et du post-traitement**



Pour les médecins demandeurs, tout professionnel de santé accédant au CR d'imagerie et/ou patients

Visualiser un examen à partir d'un lien dans le compte-rendu d'imagerie.
**Pas besoin de DRIMbox côté Consommateur*



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

1.2. Introduction à l'Espace de Confiance DRIM-M

Un compromis en matière de sécurité pour ne pas freiner l'usage métier

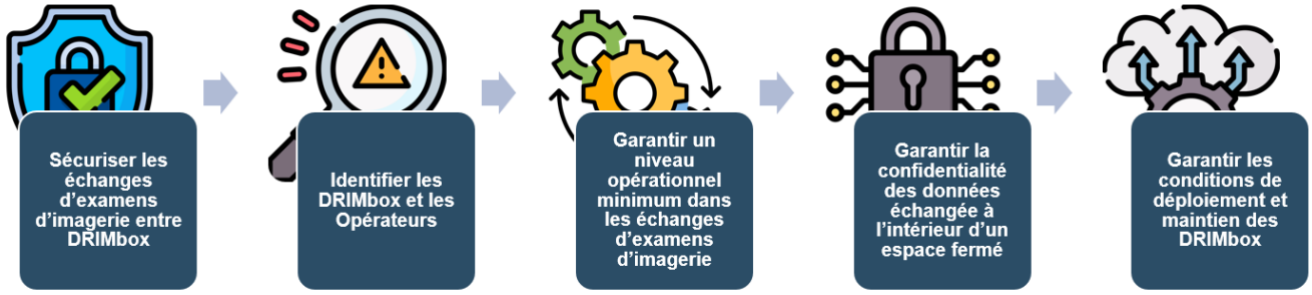
Le projet DRIM-M propose la création d'un Espace de Confiance pour **répondre aux enjeux de performance tout en assurant un niveau de sécurité optimal** pour permettre un partage fluide entre les DRIMbox.

L'**Espace de Confiance** contient :

- Un **Registre National d'identification** dont le rôle est d'assigner des noms de domaines uniques, pérennes et de confiance, gérés et distribués par l'ANS à chaque DRIMbox déployée
- Un **Domaine déposé par l'ANS** et utilisé dans le maillage DRIM-M (mesimagesmedicales.fr)
- Une **Liste Blanche** signée par l'ANS et répertoriant les DRIMbox de confiance
- Une **Météo des DRIMbox** qui permettra d'informer l'écosystème du statut opérationnel des DRIMbox

Ses objectifs

L'Espace de Confiance DRIM-M répond à cinq objectifs :



Ses acteurs

L'ANS est **l'administrateur** de l'Espace de Confiance DRIM-M.
La responsabilité de déploiement et d'intégration des DRIMbox dans l'Espace de Confiance **revient aux Opérateurs** après délégation par les Clients via la signature du document Conditions Générales d'Intégration (CGI) à l'Espace de Confiance DRIM-M.

Avant d'intégrer l'Espace de Confiance DRIM-M, **le document "Conditions Générales d'Intégration à l'Espace de Confiance DRIM-M"** doit être complété et signé par l'Opérateur souhaitant déployer la DRIMbox et ses Clients (à l'origine de la commande).

L'intégration à l'Espace de Confiance est subordonnée au respect par l'Opérateur de la procédure ci-après définie :

- *L'Opérateur doit, préalablement à toute demande d'intégration, justifier auprès de l'ANS de **l'obtention du "Référencement DRIMbox délivré par l'ANS"** en présentant une attestation de référencement en cours de validité et/ou tout autre document probant jugé suffisant par l'ANS.*
- *L'Opérateur est ensuite tenu de suivre **les étapes du parcours d'intégration** à l'Espace de Confiance en adéquation avec le présent document.*

Note : Les Clients sont des parties prenantes qui participent au déploiement des DRIMbox suivant leur périmètre d'intervention qu'ils ont défini avec l'Opérateur. Ils restent libres de changer d'Opérateur ou de retirer une DRIMbox à tout moment.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

2. L'ESPACE DE CONFIANCE

2.1. Le Registre National

Les origines de la création du Registre National

Le projet a envisagé deux options en collaboration avec l'écosystème : l'instauration d'un Registre National et la possibilité de permettre aux structures de santé de gérer leurs propres URL.

- ✓ La solution qui nous a semblé la plus appropriée pour répondre aux exigences du projet, et qui a également reçu l'adhésion des acteurs de l'écosystème, est **la création d'un Registre National d'identification des sources d'examens d'imagerie.**

Ainsi, pour chaque commande d'un site disposant d'un PACS, l'Opérateur recevra 2 URL (sous-domaines de mesimagesmedicales.fr) attribuées par l'ANS, qu'il fixera alors en dur au niveau de la DRIMbox.

Une **URL propre à la DRIMbox** de la structure émettrice, est insérée en dur dans le pointeur d'imagerie (KOS) pour lui permettre d'identifier de façon unique la DRIMbox Source. Une fois le KOS créé, il pourra alimenter le DMP du patient.	Une **URL propre à la Visionneuse** de la structure émettrice, sera ensuite insérée par le RIS producteur dans le contenu du CR d'imagerie.

Point d'attention : Cette solution est irréversible en raison de l'immuabilité de l'URL, inscrite dans le KOS et le CR.

Le **Registre National d'identification des DRIMbox Source**, géré par l'ANS, permet de créer un réseau de confiance qui regroupe l'ensemble des DRIMbox déployées avec des URL uniques, pérennes et de confiance, portées par l'ANS. Il s'agit d'un outil interne qui n'est accessible que côté ANS en tant qu'administrateur de l'Espace de Confiance DRIM-M.

Certaines données du Registre sont **communiquées à l'ANS par les Opérateurs**, d'autres sont **créées par l'ANS à destination des Opérateurs**. Les données sont mises à jour au gré des demandes et situation de DRIMbox (active, exclue, à basculer…).

Une partie des données contenues dans le Registre seront **publiées et partagées à l'écosystème dans la Liste Blanche.**

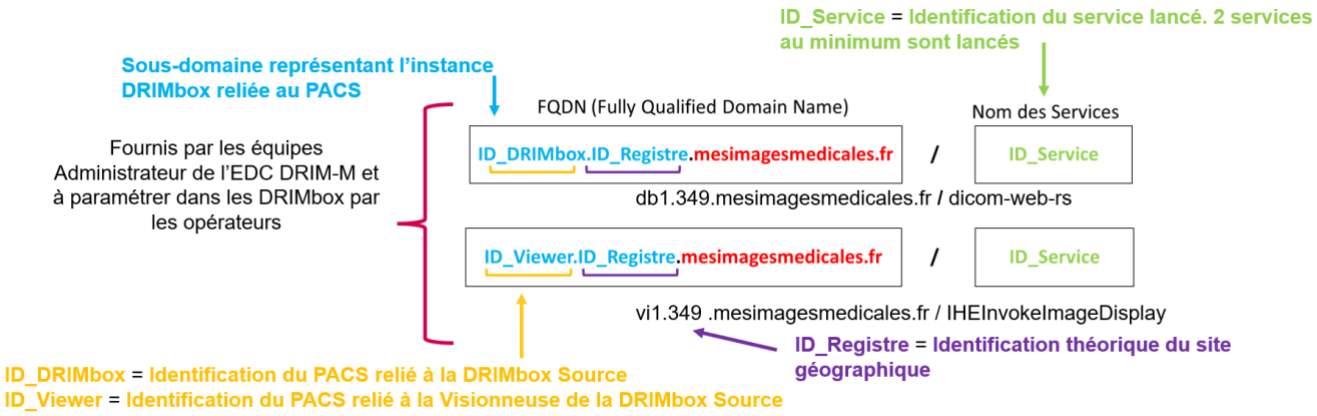
L'ANS assure **la définition et le maintien des conditions de sécurité** de ce composant de l'Espace de Confiance.

2.2. Le nom de domaine

La présentation de la structure des URL

L'ANS est propriétaire du nom de domaine **mesimagesmedicales.fr**. Ce domaine est utilisé dans le cadre du réseau DRIM-M afin d'identifier les DRIMbox déployées par les Opérateurs pour le compte des structures Clientes.
Voici la structure des URL (ou FQDN) attribuées par l'ANS :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.



Point d'attention : L'Opérateur dispose d'une autorisation d'utilisation des FQDN par les Clients lors du déploiement et maintien en conditions opérationnelles. Il est tenu de libérer les FQDN et révoquer les certificats en cas de retrait d'une DRIMbox ou bascule d'Opérateur pour une DRIMbox à la demande des Clients.

La gestion du DNS et bureau d'enregistrement

La gestion administrative du nom de domaine **mesimagesmedicales.fr** est réalisée auprès d'un bureau d'enregistrement par l'ANS.
Pour permettre la mise en œuvre de FQDN, l'équipe DRIM-M de l'ANS gère le service DNS du bureau d'enregistrement en charge de **mesimagesmedicales.fr**. Il s'agit de réaliser des **Enregistrements CNAME** reliant ainsi les FQDN aux noms d'hôte des serveurs DRIMbox source et Visionneuse source.

L'ANS assure **la définition et le maintien des conditions de sécurité** de ces composants majeurs de l'Espace de Confiance DRIM-M.

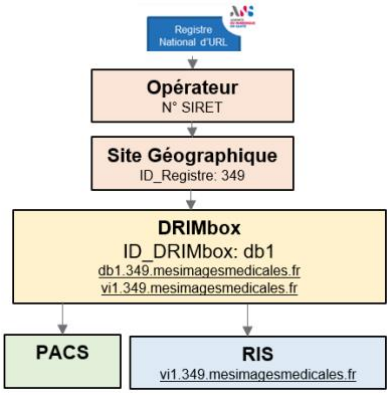
Les règles d'attribution des FQDN en fonction des architectures

L'ANS attribue N couples de FQDN (1 FQDN DRIMbox, 1 FQDN Visionneuse) si le site dispose de N PACS. Les RIS producteurs du CR doivent récupérer les FQDN des Visionneuses qui permettent d'accéder aux examens afin de les intégrer dans le contenu des CR liés à ces derniers.

Cas Simple

Dans le cas d'une installation disposant d'un RIS et d'un PACS :

- ✓ L'Opérateur communique à l'ANS du son numéro de SIRET, le SIREN et libellé du site Client.
- ✓ L'ANS fournit un ID_Registre 349 pour cette installation.
- ✓ L'Opérateur gère pour son client la DRIMbox ID_DRIMbox = db1.
- ✓ Cette DRIMbox est reliée au RIS et PACS du client.
- ✓ L'ANS attribue ces 2 FQDN
  - db1.349.mesimagesmedicales.fr
  - vi1.349.mesimagesmedicales.fr

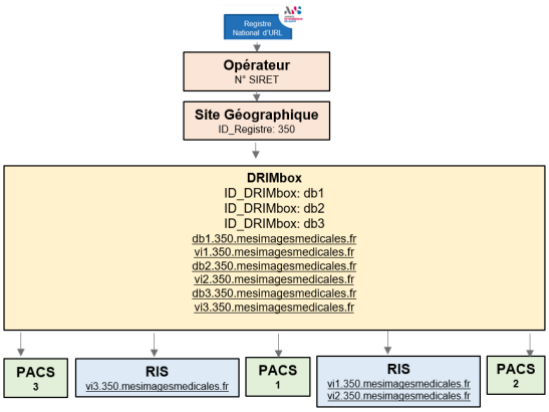


Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Cas Complexe/Mutualisé

Dans le cas d'une installation disposant de deux RIS et de trois PACS :

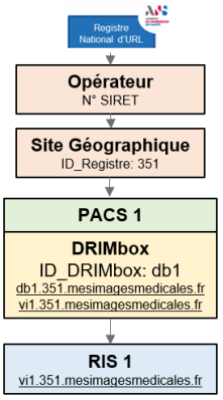
- ✓ L'Opérateur communique à l'ANS du son numéro de SIRET, le SIREN et libellé du site client.
- ✓ L'ANS fournit un ID_Registre 350 pour cette installation.
- ✓ L'Opérateur gère pour son client une DRIMbox contenant trois ID_DRIMbox = db1, db2, db3.
- ✓ Cette DRIMbox est reliée aux RIS et PACS du client.
- ✓ L'ANS attribue ces 6 FQDN
  - db1.350.mesimagesmedicales.fr
  - vi1.350.mesimagesmedicales.fr
  - db2.350.mesimagesmedicales.fr
  - vi2.350.mesimagesmedicales.fr
  - db3.350.mesimagesmedicales.fr
  - vi3.350.mesimagesmedicales.fr



Cas Natif

Dans le cas d'une installation disposant d'un RIS et d'un PACS :

- ✓ L'Opérateur communique à l'ANS du son numéro de SIRET, le SIREN et libellé du site client.
- ✓ L'ANS fournit un ID_Registre 351 pour cette installation.
- ✓ L'Opérateur gère pour son client la DRIMbox ID_DRIMbox = db1.
- ✓ Cette DRIMbox est reliée au RIS et PACS du client.
- ✓ L'ANS attribue ces 2 FQDN
  - db1.351.mesimagesmedicales.fr
  - vi1.351.mesimagesmedicales.fr



2.3. La Liste Blanche

La Liste Blanche

La Liste Blanche est un fichier XML signé par un certificat de l'ANS, contenant **la liste des Opérateurs autorisés à partager les examens d'imagerie** au sein de l'Espace de Confiance DRIM-M. Ce fichier est géré par l'ANS et mis à jour régulièrement aux grés des ajouts ou des retraits des sous-domaines autorisés au sein de l'Espace de Confiance.

Note : La section 4.11 du document [DB0] répertorie l'ensemble des exigences et spécifications associées à l'exploitation de la liste blanche ANS par un logiciel DRIMBox.

L'ANS assure **la définition et le maintien des conditions de sécurité** de ce composant de l'Espace de Confiance.

Le tableau ci-dessous présente les paramètres contenus dans la Liste Blanche des sous-domaines DRIM-M :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Champs	Description	Type	Longueur	Format
versionFormat	Version du format de la liste blanche	Alphanumérique	50	Libre
Date de Génération	Date de génération du fichier	DateTime	Sans Objet	xsd :DateTime [-] CCYY-MM-DDThh :mm :ss[Z|(+|-)hh:mm])
Sous-domaines	Liste des sous-domaines de l'Espace de Confiance DRIMbox	Liste de Domaines	Sans Objet	Liste de Domaines
Signature	Signature du fichier par l'ANS avec un certificat logiciel serveur de type ORG SIGN de l'IGC Santé	XAdES	Sans Objet	XAdES

Le champs « sous-domaines » contient les informations suivantes :

```
<?xml version="1.0" encoding="UTF-8"?>

<ListeBlancheDRIM-M xmlns="https://github.com/ansforge/DRIM-M_DATA" versionFormat="1.0.0">
    <DateDeGeneration>2025-05-20T11:08:12Z</DateDeGeneration>
    <ListeDomaines>
    <Domaine>
            <Identifiant>100</Identifiant>
            <db>db1.100.mesimagesmedicales.fr</db>
           <vi>vi1.100.mesimagesmedicales.fr</vi>
            <Denomination>ANS</Denomination>
            <DNCertificatOperateur>CN=db1.100.mesimagesmedicales.fr,OU=318751275100020,O=AGENCE DU NUMERIQUE EN SANTE,ST=Paris (75),C=FR</DNCertificatOperateur>
            <SupportContact>contactsupport@operateurdrimbox.fr</SupportContact>
            <DateMAJ>2024-12-10T11:27:12Z</DateMAJ>
        </Domaine>
        <Domaine>
            <Identifiant>100</Identifiant>
            <db>db2.100.mesimagesmedicales.fr</db>
            <vi>vi2.100.mesimagesmedicales.fr</vi>
            <Denomination>ANS</Denomination>
            <DNCertificatOperateur>CN=db2.100.mesimagesmedicales.fr,OU=318751275100020,O=AGENCE DU NUMERIQUE EN SANTE,ST=Paris (75),C=FR</DNCertificatOperateur>
            <SupportContact>contactsupport@operateurdrimbox.fr</SupportContact>
            <DateMAJ>2024-12-10T11:27:12Z</DateMAJ>
        </Domaine>
    </ListeDomaines>
</ListeBlancheDRIM-M>
```

Sa signature et sa publication

A chaque mise à jour de la Liste Blanche, l'ANS la signera. La **signature du fichier XML** de la Liste Blanche permet de vérifier son authenticité ainsi que son intégrité, c'est-à-dire :

- Qu'il a bien été émis par l'ANS ;
- Qu'il n'a pas été modifié ;
- Qu'il n'a pas été altéré.

La **vérification de la signature** doit se faire systématiquement à l'issue du téléchargement quotidien de la Liste Blanche dans le respect des exigences DRIMbox.

Ce fichier XML est **publié et accessible à l'ensemble de l'écosystème** sur Github.(ansforge/DRIM-M_liste-blanche)

L'outil **eSignSante** est un outil de signature et de vérification de signature, développé et maintenu par l'ANS pour ses propres besoins (https://github.com/ansforge/esignsante).

Il implémente **une signature enveloppée de fichier XML en XADES-Baseline B**.

Un exemple de contenu signé est donc directement visible :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

```
▼<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-49e7d621dccdc9aa806366b602da2abd">
  ▼<ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    ▼<ds:Reference Id="r-id-49e7d621dccdc9aa806366b602da2abd-1" URI="">
      ▼<ds:Transforms>
        ▼<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
           <ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
         </ds:Transform>
         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
       </ds:Transforms>
       <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
       <ds:DigestValue>z4kcESS40gtYiwcEcCIYr/gipPvJsdKJFXYBR2swCdk=</ds:DigestValue>
     </ds:Reference>
    ▼<ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-49e7d621dccdc9aa806366b602da2abd">
      ▼<ds:Transforms>
         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
       </ds:Transforms>
       <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
       <ds:DigestValue>SZ7fIIbgKpsKFY58tVGOlOqL+VKleXFbkxCf8iQiSNQ=</ds:DigestValue>
     </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue Id="value-id-
   49e7d621dccdc9aa806366b602da2abd">cROSaC7hZz8Y2AnkxAjFe7TzdJeV4xfOO6LCtTWzFVM2d82i/PGczJ9etKG3LKYcoFiT5IzUeXiVJghcXGvDJz/yyLeIfsAimx5XPuW2cxr0NFo
   </ds:SignatureValue>
  ▼<ds:KeyInfo>
    ▼<ds:X509Data>
       <ds:X509SubjectName>CN=Liste Blanche DRIM-M,OU=318751275100020,O=AGENCE DU NUMERIQUE EN SANTE,ST=Paris (75),C=FR</ds:X509SubjectName>
       <ds:X509Certificate>MIIIkDCCBnigAwIBAgIQT3d1t7VOm0srhNlHBAHuJTANBgkqhkiG9w0BAQsFADCBijELMAkGA1UEBhMCRlIxEzARBgNVBAoMCkFTSVAtU0FOVEUxFzAVBgNVBA
     </ds:X509Data>
   </ds:KeyInfo>
  ▼<ds:Object>
    ▼<xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#id-49e7d621dccdc9aa806366b602da2abd">
      ▼<xades:SignedProperties Id="xades-id-49e7d621dccdc9aa806366b602da2abd">
        ▼<xades:SignedSignatureProperties>
           <xades:SigningTime>2024-01-26T15:48:50Z</xades:SigningTime>
          ▼<xades:SigningCertificateV2>
            ▼<xades:Cert>
              ▼<xades:CertDigest>
                 <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                 <ds:DigestValue>9t3bSqvrrVX1YctUJad/iRGzB0IAtqyaTvpTdjytWgvF0e8b/qGIE4ar+Y5fdNiJUt+nzdRA3sIwU50fLI0j0A==</ds:DigestValue>
               </xades:CertDigest>
               <xades:IssuerSerialV2>MIGlMIGQpIGNMIGKMQswCQYDVQQGEwJGUjETMBEGA1UECgwKQVNJUC1TQUSURTEXMBUGA1UECwwOMDAwMiAxODc1MTI3NTExFzAVBgNVBAsNDk1H
             </xades:Cert>
           </xades:SigningCertificateV2>
         </xades:SignedSignatureProperties>
        ▼<xades:SignedDataObjectProperties>
          ▼<xades:DataObjectFormat ObjectReference="#r-id-49e7d621dccdc9aa806366b602da2abd-1">
             <xades:MimeType>application/octet-stream</xades:MimeType>
           </xades:DataObjectFormat>
         </xades:SignedDataObjectProperties>
       </xades:SignedProperties>
     </xades:QualifyingProperties>
   </ds:Object>
 </ds:Signature>
</ListeBlancheDRIM-M>
```


2.4. La météo des services

Le service **« Status » https://status.drimm.esante.gouv.fr** (outil Better Uptime) est étendu dans le cadre du projet DRIM-M afin d'apporter une vision globale de l'état opérationnel du maillage DRIM-M. Pour intégrer ce service de supervision, la DRIMbox doit permettre la remontée d'informations concernant son statut, via **un service « HealthCheck » décrit dans les spécifications DRIMbox**. L'ANS ajoutera les données associées à la DRIMbox et son PACS dans l'outil **Better Uptime**. Le service « Status » réalisera des **HealthChecks** (Pings) quotidiens sur des URL exposées par des APIs hébergées au sein du SI de l'ANS (Ups/Downs). L'ANS assure **la définition et le maintien des conditions de sécurité** de ce composant de l'Espace de Confiance.	

2.5 Les certificats

Un certificat **logiciel** est un fichier informatique faisant fonction de pièce d'identité numérique. Il permet 3 fonctionnalités principales :

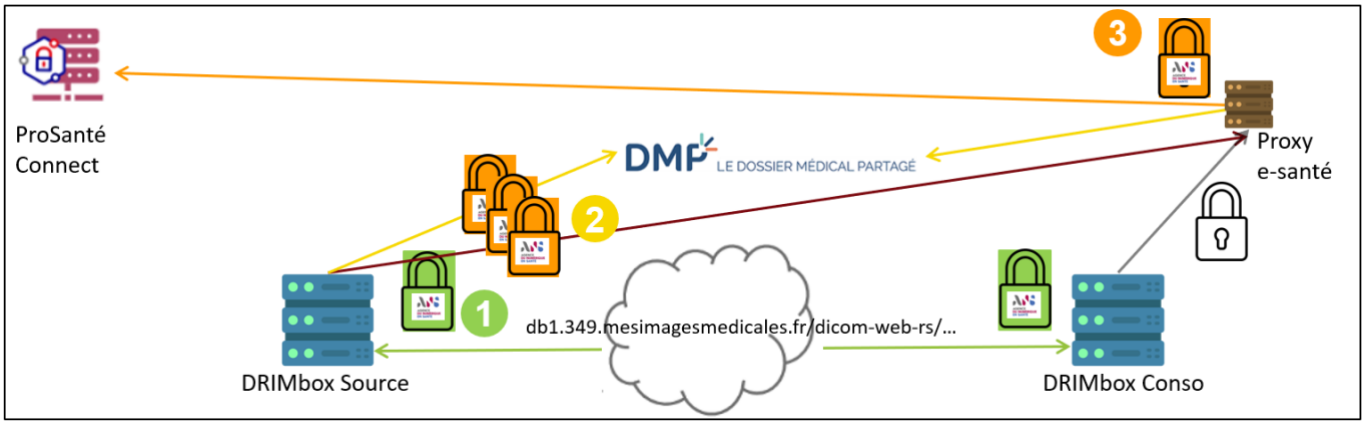
- l'authentification ;
- la signature électronique ;
- la sécurisation / le chiffrement des données.

Le besoin en certificat IGC-Santé

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Produit	Position	Usage
SERV_SSL	sur la DRIMbox dont le rôle est Source et Conso	Sécurisation des échanges entre DRIMbox. (La clé publique des certificats de l'IGC Santé est non reconnue automatiquement par les navigateurs mais cela n'est pas bloquant ces échanges sont réalisés en backend entre DRIMbox.)
ORG AUTH_CLI et ORG SIGN	sur la DRIMbox Source	Alimentation et signature des lots de soumissions au DMP. Ce couple de certificats est raccroché à la situation d'exercice du PS dont le besoin est d'alimenter le DMP. Il y a donc 1 à n couple de certificats (1 ORG AUTH_CLI et 1 ORG SIGN) pour 1 à n situations d'exercice qui correspondent aux structures.
ORG AUTH_CLI	sur le Proxy e-santé	Sécurisation des échanges Proxy e-santé avec les endpoints PSC et DMP. 1 certificat par Opérateur de DRIMbox. Contenu : CN : Client ID de l'Opérateur de DRIMbox, OU : ID Nat Struct du proxy Opérateur

Note : Il est nécessaire de sécuriser le lien entre DRIMbox et Proxy e-santé suivant le référentiel PSC Espace de Confiance.

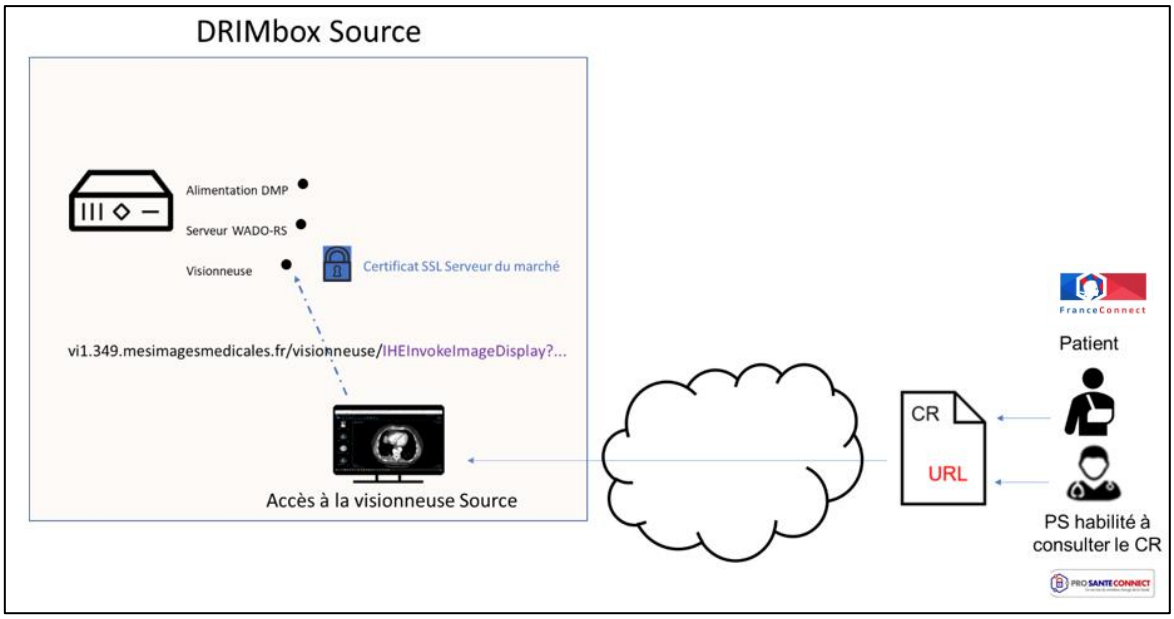


*« Les prestations d'accompagnement **[du Client par l'Opérateur DRIMbox]** à l'obtention d'un à plusieurs certificats logiciels de type organisation auprès de l'autorité de certification de référence, l'IGC Santé, pour les services d'imagerie n'en disposant pas déjà, ainsi que l'implémentation de ce certificat sur les infrastructures adéquates ; »* sont prévus dans l'Appel à Financement de la DRIMbox Ségur Vague 2.

Le besoin en certificat du marché

Produit	Position	Usage
SSL	sur la DRIMbox Source	Sécuriser les échanges entre la DRIMbox Source et le lien URL sur le CR. (La clé publique des certificats de l'IGC Santé est non reconnue automatiquement par les navigateurs.)

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.



L'Opérateur doit commander **un certificat SSL du marché de niveau OV au minimum**. Une liste des Autorités de certification de confiance est présente sur [La liste nationale de confiance | ANSSI].

Les cas spécifiques suivants illustrent le besoin en certificat :

Cas Natif

Dans le cas d'une installation disposant de 2 RIS et 1 PACS pour 1 opérateur DRIMbox :

- ✓ Cette DRIMbox est reliée aux RIS et PACS du client.
- ✓ L'ANS attribue ces 2 FQDNs
  - db1.350.mesimagesmedicales.fr
  - vi1.350.mesimagesmedicales.fr

Le besoin en certificat est le suivant

- 1 SERV_SSL IGC-Santé
- 1 à N en fonction des situations d'exercice (ORG AUTH_CLI et ORG SIGN)
- 1 ORG AUTH_CLI (Proxy e-santé)
- 1 SSL du marché
- Il est nécessaire de sécuriser le lien entre DRIMbox et Proxy e-santé suivant le référentiel PSC Espace de Confiance.

Cas Simple

Dans le cas d'une installation disposant de 1 RIS et 1 PACS pour une commande Client #A DRIMbox :

- db1.349.mesimagesmedicales.fr
- vi1.349.mesimagesmedicales.fr

Le besoin en certificat est le suivant

- 1 SERV_SSL IGC-Santé
- 1 à N en fonction des situations d'exercice (ORG AUTH_CLI et ORG SIGN)
- 1 ORG AUTH_CLI (Proxy e-santé)
- 1 SSL du marché
- Il est nécessaire de sécuriser le lien entre DRIMbox et Proxy e-santé suivant le référentiel PSC Espace de Confiance.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Cas Complexe : pour plusieurs commandes de clients différents avec 1 opérateur qui a une DRIMbox mutualisée pour tous ces clients

Dans le cas d'une installation disposant de 2 RIS et 3 PACS pour une commande Client #B DRIMbox :

- db1.350.mesimagesmedicales.fr
- vi1.350.mesimagesmedicales.fr
- db2.350.mesimagesmedicales.fr
- vi2.350.mesimagesmedicales.fr
- db3.350.mesimagesmedicales.fr
- vi3.350.mesimagesmedicales.fr

Le besoin en certificat est le suivant

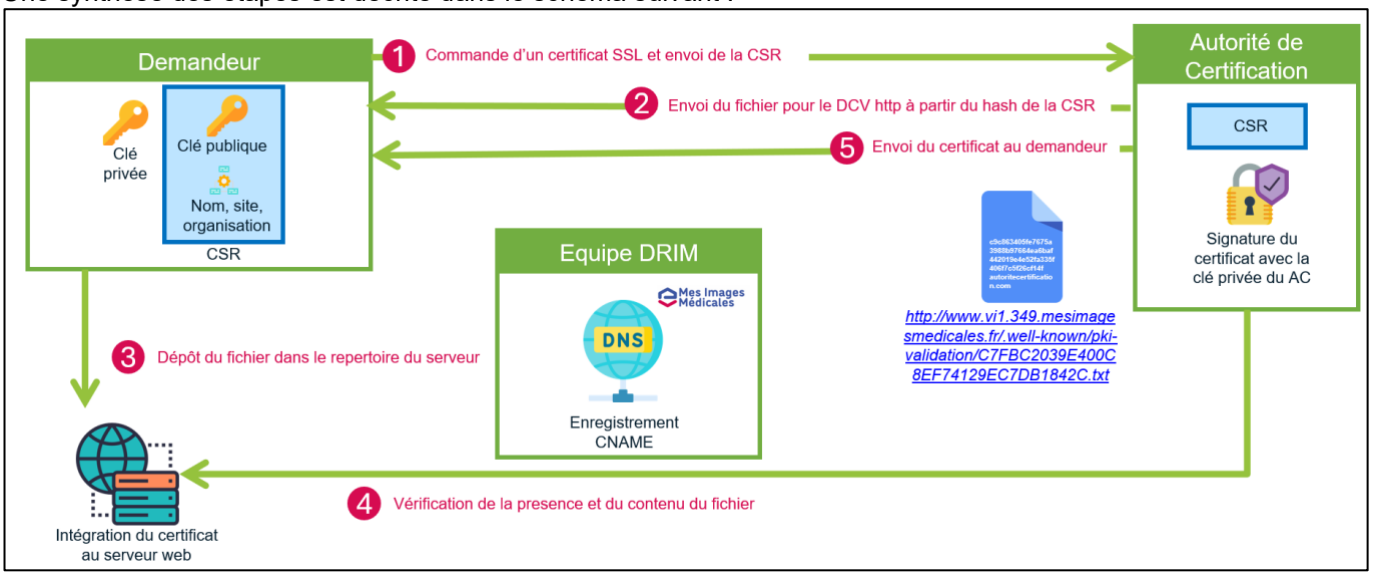
- 3 SERV_SSL IGC-Santé
- 1 à N en fonction des situations d'exercice et des activité (ORG AUTH_CLI et ORG SIGN)
- 1 ORG AUTH_CLI (Proxy e-santé)
- 3 SSL du marché
- Il est nécessaire de sécuriser le lien entre DRIMbox et Proxy e-santé suivant le référentiel PSC Espace de Confiance.

2.5. La validation du contrôle de domaine

Afin d'obtenir un certificat SSL du marché pour les FQDN distribués par l'ANS, l'Opérateur doit disposer d'un accord du propriétaire du domaine à sécuriser. Ce processus se nomme **« Validation du contrôle de domaine » (Domain Control Validation, DCV).**

Le challenge DCV permet de prouver l'accord du propriétaire du nom de domaine avant de recevoir les certificats. Il s'appuie sur l'enregistrement CNAME réalisé par l'équipe DRIM-M sur le DNS, une CSR (Certificate Signing Request) et un fichier de validation.

Une synthèse des étapes est décrite dans le schéma suivant :



En complément du challenge DCV qui assure le contrôle du domaine, l'Autorité de certification vérifie l'existence de l'organisation qui demande le certificat pour délivrer un certificat SSL de niveau OV ou RGS*.

2.6 L'automatisation de la gestion des certificats

L'automatisation de la gestion des certificats IGC-Santé

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

L'IGC-Santé est la plateforme de référence opérée par l'ANS pour la **gestion des certificats électroniques dans le domaine de la santé**. Elle permet aux organisations (personnes morales) de :

- gérer l'ensemble du **cycle de vie** des certificats (demande, renouvellement, révocation) ;
- retirer des **certificats logiciels pour leurs applications ou serveurs** ;
- disposer d'une **interface centralisée et sécurisée**, réservée aux **administrateurs techniques habilités**.

Deux options sont possibles en matière d'automatisation :

- Les certificats sont commandés par l'Opérateur auquel le Client délègue la gestion complète des certificats. Ainsi, l'Opérateur doit gérer ses propres certificats en son nom.

Les certificats sont commandés, de façon automatique, par le Client, à travers un module mis à disposition par l'Opérateur. Cette option est envisageable pour les certificats ORG du DMP.

Usage de l'API IGC-Santé

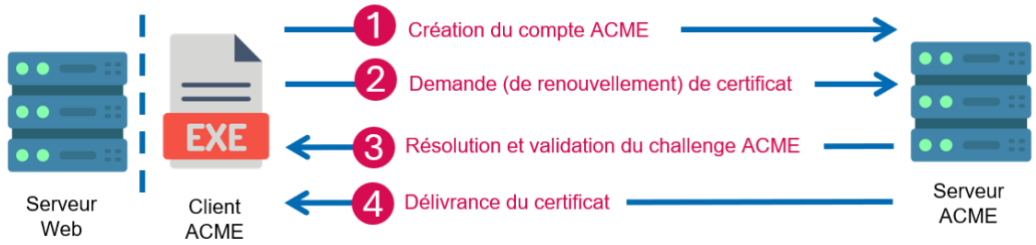
- ✓ Ce guide permet à tout éditeur de développer un module qui utilise l'API IGC Santé pour proposer le téléchargement, l'installation et le renouvellement automatique des certificats. https://industriels.esante.gouv.fr/sites/default/files/media/document/ANS_IGC-Sante_Guide-WebService_v1.1.0.pdf
  Generation-du-CSR

Note : Une évolution intégrant les **protocoles ACME** est prévue pour T4 2025.

L'automatisation de la gestion des certificats du marché

Le protocole ACME (Automatic Certificate Management Environment) est une méthode qui automatise l'obtention et le renouvellement de certificats de sécurité SSL. Il permet de répondre aux futures exigences des navigateurs qui visent à raccourcir la durée de vie des certificats.

Usage du protocole ACME et son client



- ✓ « Une fois la création de compte réalisée et associée, la demande (ou le renouvellement) de certificats, la résolution de challenge ACME et la réception de certificat peuvent être complètement automatisées pour le demandeur de certificats. » Le schéma ci-dessus, résume ces étapes.
- ✓ Le document suivant fournit des recommandations pour sécuriser cette automatisation. Automatisation de la gestion des certificats avec ACME | ANSSI
- ✓ L'équipe DRIM-M a ajouté deux conditions dans les CGI en lien avec l'automatisation
  - Gérer la purge sur le serveur Web des anciens fichiers utilisés dans le cadre de l'obtention des certificats
  - Sécuriser l'usage de client (tel qu'ACME par exemple) pour automatiser la gestion des certificats

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.