



# Guide commande de certificats

SEGUR - Couloir médico-social – V0.6

**12/12/2022**

*Guide à destination des éditeurs, des GRADeS et des  
Établissements et Services Sociaux ou Médico-Sociaux*

# Sommaire



- Résumé du document [3](#)
- Règles et cas concrets de gestion des certificats du couloir médico-social [7](#)
- Démarche d'obtention des certificats [14](#)
- Les futures évolutions [39](#)
- Annexes [41](#)

# Résumé du document



## Résumé du document : les certificats, prérequis nécessaires aux établissements pour accéder aux services et référentiels du Ségur

Le Ségur numérique accélère le déploiement de la feuille de route du numérique en santé : il nécessite des **prérequis d'identification électronique** pour les professionnels de santé, les professionnels du social et médico-social et les **structures de santé dont des certificats**. Ils sont indispensables pour **sécuriser l'identification électronique de personnes morales à des services numériques en santé tels que l'alimentation du DMP et l'appel au téléservice INSi**.

Un certificat logiciel est un fichier informatique faisant fonction de **pièce d'identité numérique**. Il permet de **garantir à distance l'identité d'une personne morale** (une structure médico-sociale par exemple) pour l'accès à des services numériques en santé. Dès lors qu'un certificat est mis en œuvre, les professionnels de la structure peuvent interagir avec les services sans moyens d'identification personnels (il n'y a pas besoin de cartes CPS pour alimenter le DMP ou consulter l'INS). Un certificat logiciel contient des informations sur son propriétaire, certifiées par un tiers de confiance appelé "autorité de certification". Il permet 3 fonctionnalités principales :



**L'authentification**



**La signature électronique**



**La sécurisation / le chiffrement des données**

**L'Agence du Numérique en Santé est l'autorité de certification du domaine de la santé.** Elle délivre des certificats logiciels via **le formulaire 413** pour sécuriser les échanges de données de santé informatisés entre les professionnels de santé, du social et médico-social exerçant en ville, à l'hôpital et dans les établissements médico-sociaux

L'ANS délivre **ces certificats, via son autorité de certification IGC-Santé.**

L'ANS simplifie l'obtention des certificats pour le secteur médico-social autour de 5 principes clés :

- 1** Les certificats peuvent être commandés avec le numéro FINESS de l'entité juridique pour l'ensemble des établissements géographiques rattachés (dans l'hypothèse où les établissements géographiques utilisent le même système d'information). Dans le cas où tous les établissements géographiques n'utilisent pas le même système d'information, **il faut disposer de certificats distincts pour chaque instance logicielle**. Cependant, ces certificats peuvent utiliser le même identifiant FINESS juridique.
- 2** Les **groupements d'organismes gestionnaires** ne peuvent disposer d'un unique certificat, ils **doivent commander un certificat pour chaque entité juridique. Il n'est pas non plus possible d'utiliser un certificat au nom de l'éditeur.**
- 3** **Le certificat d'une structure peut être utilisé pour plusieurs services** (ex: alimentation DMP, échange entre logiciel métier et opérateur de MSSanté, etc.), à l'exception du téléservice INSi **qui a besoin de son propre certificat**. Ainsi l'ESSMS doit disposer a minima de **trois certificats** : deux certificats pour alimenter le DMP (un certificat pour signature et un certificat pour authentification) et un certificat pour le téléservice INSi.
- 4** **Les éditeurs peuvent réaliser les démarches pour le compte de leurs clients**, s'ils obtiennent une délégation. Ils peuvent ainsi jouer **le rôle d'administrateur technique** pour générer et implémenter les certificats
- 5** Tous les ESSMS ayant déjà déployés les certificats EG pour le DMP et l'INSi peuvent **conserver leurs certificats actuels** et migreront vers les certificats EJ lors du renouvellement de certificat (tous les trois ans).



Cliquer sur l'icône pour accéder aux détails des certificats



Cliquer sur l'icône pour accéder aux détails des catégories de certificats



Cliquer sur l'icône pour accéder aux détails de l'alimentation du DMP

La démarche d'obtention des certificats peut être réalisée par l'OG ou déléguée à un éditeur. Cette démarche nécessite la mise en place de **prérequis et l'habilitation d'un administrateur technique (via le formulaire 413) qui procédera à l'installation du ou des certificat(s)**. Elle se déroule en 4 étapes :

### Etape 1

L'OG **contractualise avec l'ANS** sous le numéro **FINESS juridique**

### Etape 2

L'OG **désigne l'administrateur technique** (dans sa structure ou délègue à son éditeur)

### Etape 3

L'éditeur ou l'OG **fait la demande de certificat** (à l'ANS via le formulaire 413 signé par le représentant légal de l'OG)

### Etape 4

Après validation par l'ANS du formulaire 413, **l'administrateur se connecte avec sa carte sur la plateforme IGC Santé** pour télécharger les certificats, qu'il peut alors installer sur l'instance logicielle dont il a la charge

# Règles et cas concrets de gestion des certificats pour les structures médico-sociales



Le terme d'entité recouvre deux notions différentes :



**Entité juridique (EJ)** : elle correspond à la notion de personne morale (ou organisme gestionnaire). Elle est identifiée par un N° FINESS juridique. **Une ou plusieurs entité(s) géographique(s) peuvent être rattaché(s) à une entité juridique.**



**Entité géographique (EG)** : elle correspond à une implantation géographique. **Chaque EG est rattachée à une seule entité juridique.** Ces entités sont identifiées par un N° FINESS Géographique.

### Règle de commande des certificats

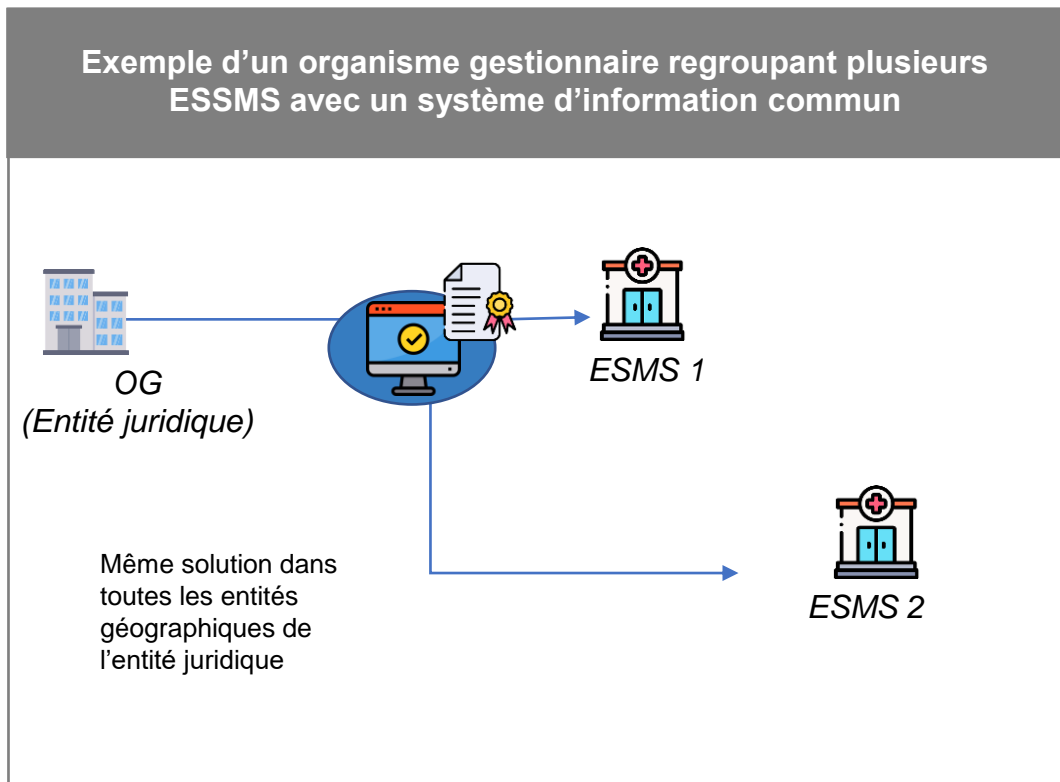
**Les certificats peuvent être commandés au niveau de l'entité juridique** pour l'ensemble des établissements géographiques dans l'hypothèse d'un système d'information unifié. Dans le cas où tous les établissements géographiques n'utilisent pas le même système d'information, **il faut disposer de certificats distincts pour chaque instance logicielle.** Cependant, ces certificats peuvent être commandé sous le même identifiant FINESS juridique.

Les **groupements d'organismes gestionnaires** ne peuvent disposer d'un unique certificat, ils **doivent commander un certificat pour chaque entité juridique.** Il n'est pas non plus possible d'utiliser un certificat au nom de l'éditeur.

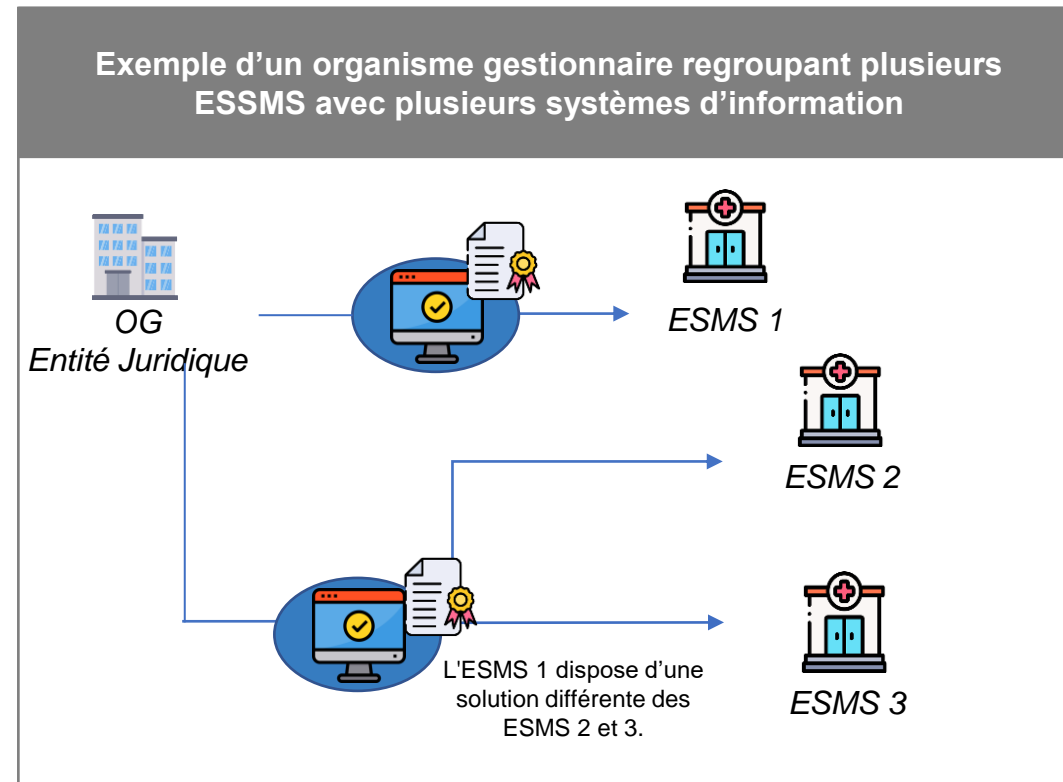
**Le certificat d'une structure peut être utilisé pour plusieurs services** (ex: alimentation DMP, échange entre logiciel métier et opérateur de MSSanté, etc.), à l'exception du téléservice INSi **qui a besoin de son propre certificat.** Ainsi l'ESSMS doit disposer a minima de **trois certificats** : deux certificats pour alimenter le DMP (un certificat pour signature et un certificat pour authentification) et un certificat pour le téléservice INSi.



• Application des règles relatives au couloir médico-social



**Un seul certificat porté par le FINESS juridique de l'organisme gestionnaire est nécessaire et suffisant** pour que l'ensemble des ESSMS puissent accéder aux services et référentiels socles.

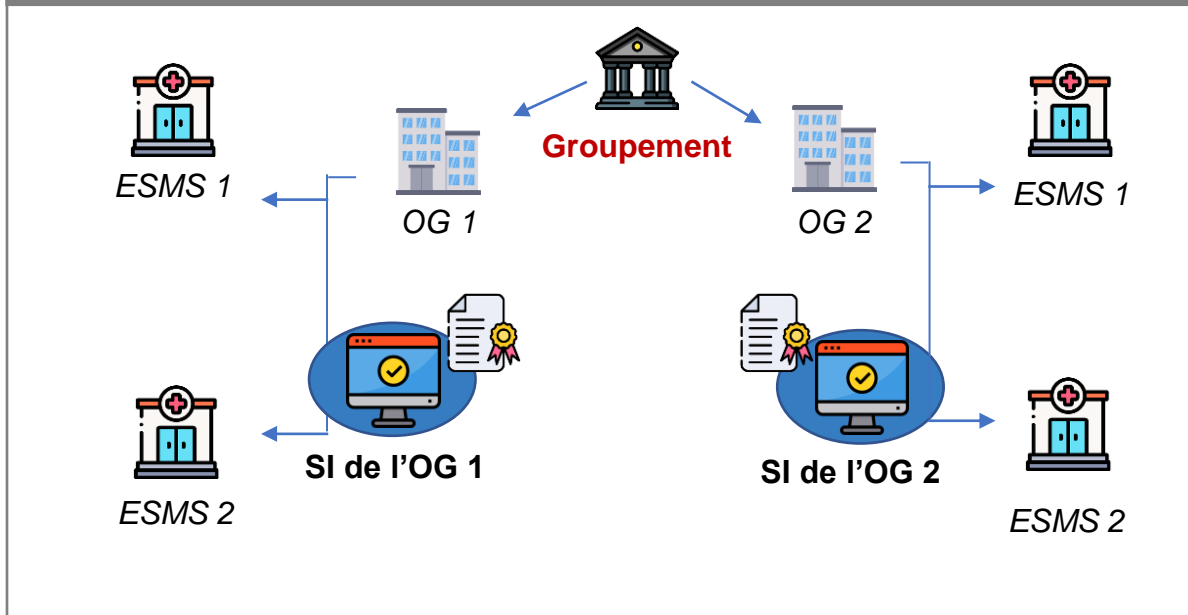


L'organisme gestionnaire ne dispose pas d'un système d'information unifié. Plusieurs solutions (DUI,...) ont été déployées dans différents ESSMS. Ainsi, **chaque solution doit disposer de son propre certificat associé au même FINESS juridique :**

- un certificat pour la solution de l'ESMS 1
- un autre certificat pour la solution des ESMS 2 et 3

• Application des règles relatives au couloir médico-social

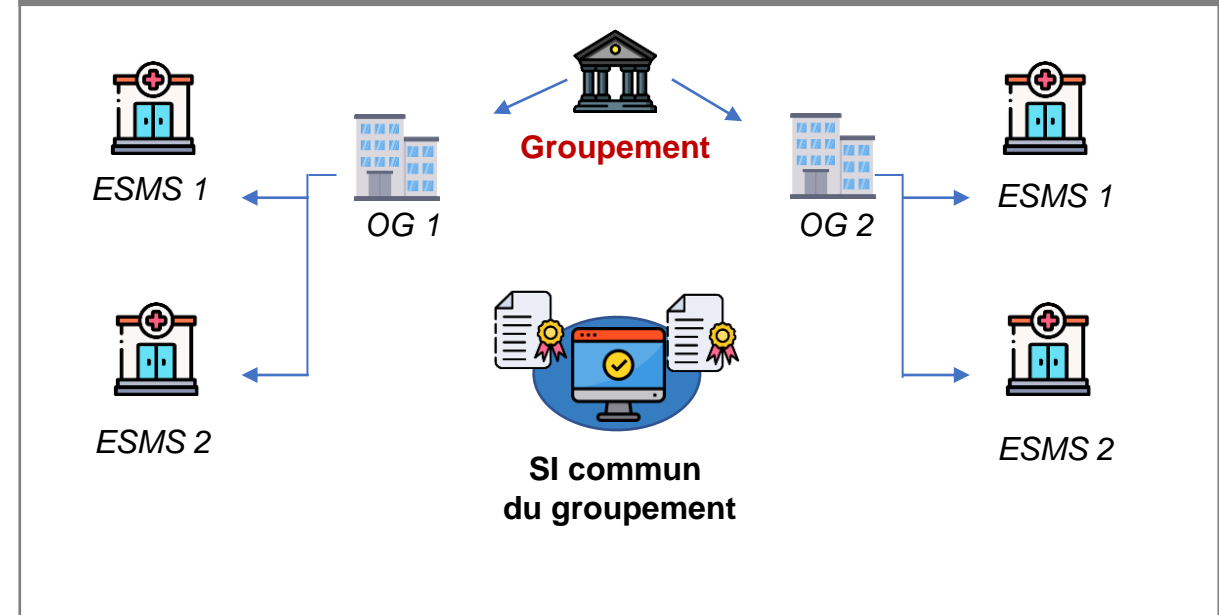
Exemple d'un groupement regroupant plusieurs organismes gestionnaires et plusieurs ESSMS avec un système d'information propre à chaque OG



Chacun OG commande son propre certificat personne morale pour sa solution.

Dans ces 2 cas, le groupement n'étant pas **la plus petite entité juridique**, il est nécessaire que **chaque organisme gestionnaire puisse disposer d'un certificat (FINESS EJ)**. Ainsi le groupement doit disposer **d'autant de certificats que d'organisme gestionnaire**.

Exemple d'un groupement regroupant plusieurs organismes gestionnaires et plusieurs ESSMS avec un système d'information unique au sein du groupement







Lorsque le groupement dispose d'un SI commun pour l'ensemble des OG, **le SI commun doit être en capacité de gérer plusieurs certificats personnes morales**. Chaque OG doit disposer son propre certificat



- Un seul type de certificat (ORG) pour accéder aux services socles du SEGUR

Un certificat d'organisation est un **certificat électronique qui joue le rôle de carte d'identité pour la structure sanitaire / médico-sociale / sociale**. Son propriétaire est une **personne morale**.

L'accès aux services numériques Ségur implique que chaque ESSMS dispose, a minima, des certificats suivants :

	Projets / usages	Certificats	Commentaires / particularités
Service SEGUR	 Pour l'alimentation du DMP	<ul style="list-style-type: none"> <li>• <b>ORG SIGN</b> – signature électronique des documents avant envoi</li> <li>• <b>ORG AUTH_CLI</b> – authentification auprès du DMP lors de l'alimentation</li> </ul>	<ul style="list-style-type: none"> <li>• 2 certificats sont nécessaires, pas de nommage particulier</li> </ul>
	 Pour l'accès au téléservice INSi	<ul style="list-style-type: none"> <li>• <b>ORG AUTH_CLI</b> – authentification auprès du téléservice INSi</li> </ul>	<ul style="list-style-type: none"> <li>• Le nommage* du certificat doit respecter les conventions prévues au guide d'intégration INSi (INSI-MANU / INSI-AUTO) selon le type d'appels</li> </ul>
	 Pour s'accorder à Pro Santé Connect	<ul style="list-style-type: none"> <li>• <b>ORG AUTH_CLI</b> – authentification mutuelle entre l'application (à s'accorder) et le ProSanté Connect</li> </ul>	<ul style="list-style-type: none"> <li>• Pas de nommage particulier, concerne uniquement les fournisseurs de service raccordé au PSC</li> </ul>
	 Pour sécuriser les échanges via la Messagerie Sécurisée de Santé	<ul style="list-style-type: none"> <li>• <b>ORG AUTH_CLI</b> – authentification du porteur de la BAL applicative</li> <li>• <b>SERV SSL</b> – sécurisation de l'espace de confiance pour les opérateurs</li> </ul>	<ul style="list-style-type: none"> <li>• Pas de nommage particulier pour le certificat ORG</li> <li>• Rappel : Le certificat SSL est obligatoire uniquement pour les opérateurs</li> </ul>

Les certificats organisations utilisés peuvent aussi permettre d'accéder à d'autres services (ROR, ROC...).

## Doctrine en cible



### *Pour les établissements du secteur social et médico-social*

- **Pour l'implémentation du certificat : Un certificat porté par l'entité juridique** (sous le numéro FINESS EJ) peut être implémenté pour l'alimentation du DMP de l'ensemble des établissements géographiques.
- **Pour la traçabilité du DMP : Le FINESS géographique doit être renseigné dans les métadonnées du DMP** dans le jeton du VIH, dans le lot de soumission et dans le document (CDA, XDS)



### *Perspective calendaire*

- **Cette nouvelle doctrine sera applicable à partir de avril 2023**. La date effective sera communiquée ultérieurement, elle est liée aux évolutions du DMP visant à remplacer le contrôle d'égalité stricte entre l'identifiant structure du jeton VIH et celui porté dans le certificat, par un contrôle de cohérence (les numéros FINESS doivent appartenir à la même entité juridique).
- A noter, **le renseignement des FINESS géographiques lors de l'alimentation du DMP** (VIH, lot de soumission et document) **sera rendu obligatoire vers la fin d'année 2023**.



### A court terme

- **Pour ceux qui alimentent déjà le DMP avec les certificats que ce soit EG ou EJ, vous pouvez conserver le fonctionnement actuel** et migrer vers la configuration de la doctrine en cible d'ici fin 2023.
- **Pour ceux qui doivent implémenter les certificats pour l'alimentation du DMP**, en attendant l'évolution du DMP, vous avez le choix entre :

**Implémenter N certificats sous le FINESS EG pour vos N établissements géographiques, et renseigner le FINESS EG dans les métadonnées DMP** dans le jeton du VIHf, dans le lot de soumission et dans le document (CDA, XDS)

**Implémenter 1 certificat juridique et renseigner le FINESS EJ dans les métadonnées DMP** dans le jeton du VIHf, dans le lot de soumission et dans le document (CDA, XDS) en attendant l'évolution du DMP.



Les métadonnées DMP sont configurées sous FINESS géographique comme demandé dans le schéma cible



Gestion d'un seul certificat (une seule démarche à réaliser)



Implémenter plusieurs certificats (N contrats, N cartes administrateurs techniques, N formulaires 413...)

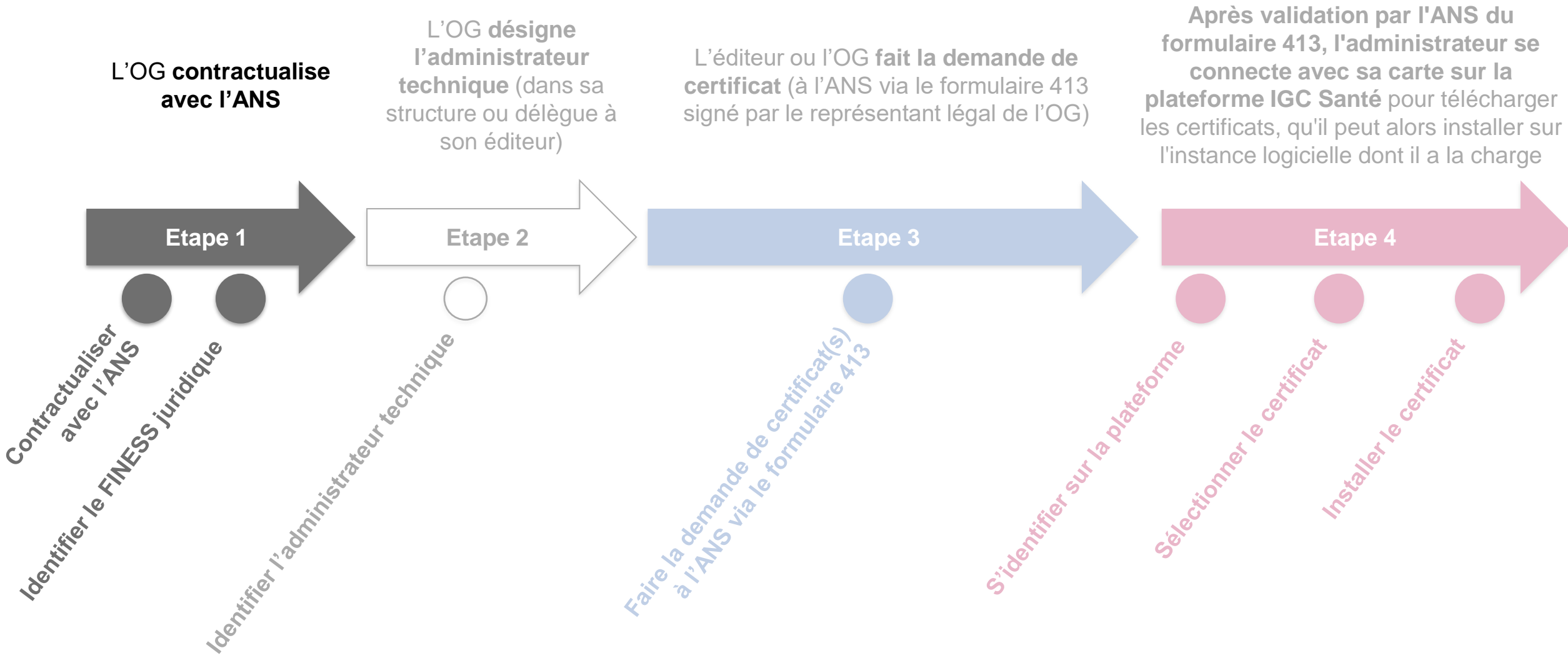


Reconfiguration de la métadonnée DMP (FINESS EG à la place du FINESS EJ) en 2023.  
Les statistiques ne pourront se faire qu'à la maille juridique et non géographique

# Démarche d'obtention des certificats

• Démarche d'obtention des certificats : L'OG contractualise avec l'ANS

Le schéma ci-dessous présente les différentes étapes nécessaires à l'obtention d'un certificat



• Etape 1 : L'OG contractualise avec l'ANS

Le schéma ci-dessous présente les différentes actions nécessaires à l'étape 1

Etape 1

Contractualiser avec l'ANS  
Identifier le FINESS Juridique

L'OG souscrit un contrat d'adhésion aux services de l'ANS pour disposer des MIE (certificats, cartes)



Le contrat avec l'ANS s'effectue en cliquant sur le lien suivant  
<https://esante.gouv.fr/nod/e/2683>

L'OG dispose d'un contrat sur son FINESS juridique



Le représentant légal a déjà une CPS (est un professionnel de santé) ?

Oui

Etape 2

Non

Une carte de représentant légal (CDE) est nécessaire



La demande de carte à l'ANS s'effectue via le formulaire 101  
<https://esante.gouv.fr/documents/101>

Le représentant légal reçoit sa carte CDE



Etape 2



● Etape 1 : Contractualiser avec l'ANS

La commande de certificats nécessite que l'OG ait souscrit un contrat d'adhésion avec l'ANS et dispose d'une carte de Directeur de l'établissement

Valider la souscription d'un contrat entre l'OG et l'ANS



Validez que l'OG choisi a déjà contractualisé avec l'ANS.

La contractualisation de l'OG avec l'ANS s'effectue au niveau du **FINESS juridique**.

Si un contrat d'adhésion existe déjà entre l'ANS et l'OG (réalisé au cours d'autres projets), il n'est pas nécessaire de re-contractualiser.

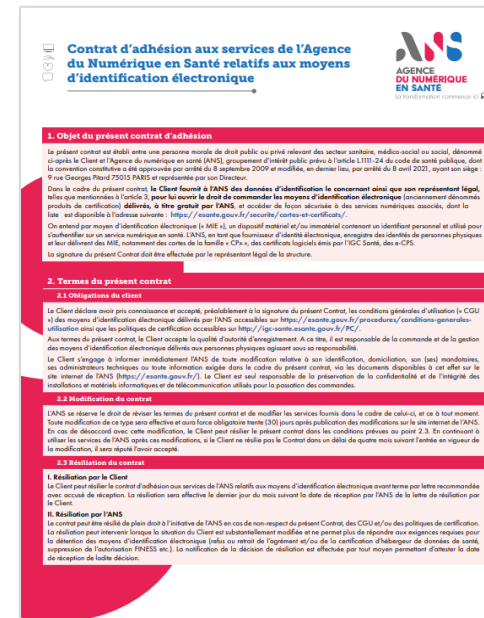


Validez que l'OG dispose d'une carte de Directeur d'Etablissement (CDE)

La démarche de contractualisation peut être réalisée en ligne via le lien ci-contre : <https://www.demarches-simplifiees.fr/commencer/contrat-d-adhesion-f101>

LE CONTRAT D'ADHÉSION

Contrat d'adhésion aux services de l'ANS relatifs aux moyens d'identification électronique est accessible au téléchargement au lien suivant : <https://esante.gouv.fr/node/2683>



LE REPRÉSENTANT LÉGAL

Le formulaire de commande 101 de commande de carte pour le Directeur d'établissement est accessible au téléchargement au lien suivant : <https://esante.gouv.fr/documents/101>



• Etape 1 : Identifier le FINESS juridique

La commande de certificats nécessite que **l'établissement renseigne son FINESS juridique.**

L'information relative au FINESS juridique est disponible sur le site : [finess.sante.gouv.fr](http://finess.sante.gouv.fr)

Indiquer la **raison sociale** d'un établissement membre de l'OG

N° FINESS - RAISON SOCIALE / ADRESSE	CATEGORIE
060024411 CHU DE NICE ANTENNE SMUR SITE HPNCL 57 AVENUE DE LA CALIFORNIE 06000 NICE Tél : 04 92 03 03 00	[101] Centre Hospitalier Régional (C.H.R.)
<b>060785003 CHU DE NICE HOPITAL PASTEUR 30 AVENUE DE LA VOIE ROMANE 06000 NICE Tél : 04 92 03 76 09</b>	[101] Centre Hospitalier Régional (C.H.R.)
060923151 CSAPA CHU DE NICE 4 AVENUE REINE VICTORIA 06001 NICE CEDEX 1	[191] Centre soins accompagnement prévention addictologie (CSAPA)
060788957 CHU DE NICE HOPITAL DE CIMIEZ 4 AVENUE REINE VICTORIA 06003 NICE CEDEX 1 Tél : 04 92 03 44 22	[101] Centre Hospitalier Régional (C.H.R.)
060793775 CHU DE NICE SLD DE L'HOPITAL DE CIMIEZ 4 AVENUE REINE VICTORIA 06003 NICE CEDEX 1 Tél : 04 92 03 44 44	[362] Etablissement de Soins Longue Durée
060790573 CHU DE NICE CTRE CONSULT TRAIT DENT 5 RUE PIERRE DEVOLUY 06006 NICE CEDEX 1 Tél : 04 92 03 45 03	[101] Centre Hospitalier Régional (C.H.R.)
060789195 CHU DE NICE HOPITAL DE L'ARCHET 151 ROUTE SAINT ANTOINE DE GINESTIERE 06200 NICE Tél : 04 92 03 55 25	[101] Centre Hospitalier Régional (C.H.R.)
060789799 CAMSP CHU DE NICE 52 AVENUE DENIS SEMERIA 06300 NICE Tél : 04 92 03 60 77	[190] Centre Action Médico-Sociale Précoce (C.A.M.S.P.)
060016508 CENTRE DE FORMATION DU CHU DE NICE 10 AVENUE BANCO 06300 NICE Tél : 04 92 03 21 20	[300] Ecoles Formant aux Professions Sanitaires
060004538 ECOLE DE SAGES FEMMES CHU DE NICE 10 AVENUE BANCO 06300 NICE Tél : 04 92 03 21 00	[300] Ecoles Formant aux Professions Sanitaires
060789245 CHU DE NICE HOP ANNEXE DE CANTARON 254 CHEMIN DE LA LAUVETTE 06340 CANTARON Tél : 04 93 54 99 70	[101] Centre Hospitalier Régional (C.H.R.)
060790177 CHU DE NICE CTRE CONVALESCENCE TENDE 3 RUE JEAN MEDECIN 06430 TENDE Tél : 04 93 03 50 00	[101] Centre Hospitalier Régional (C.H.R.)

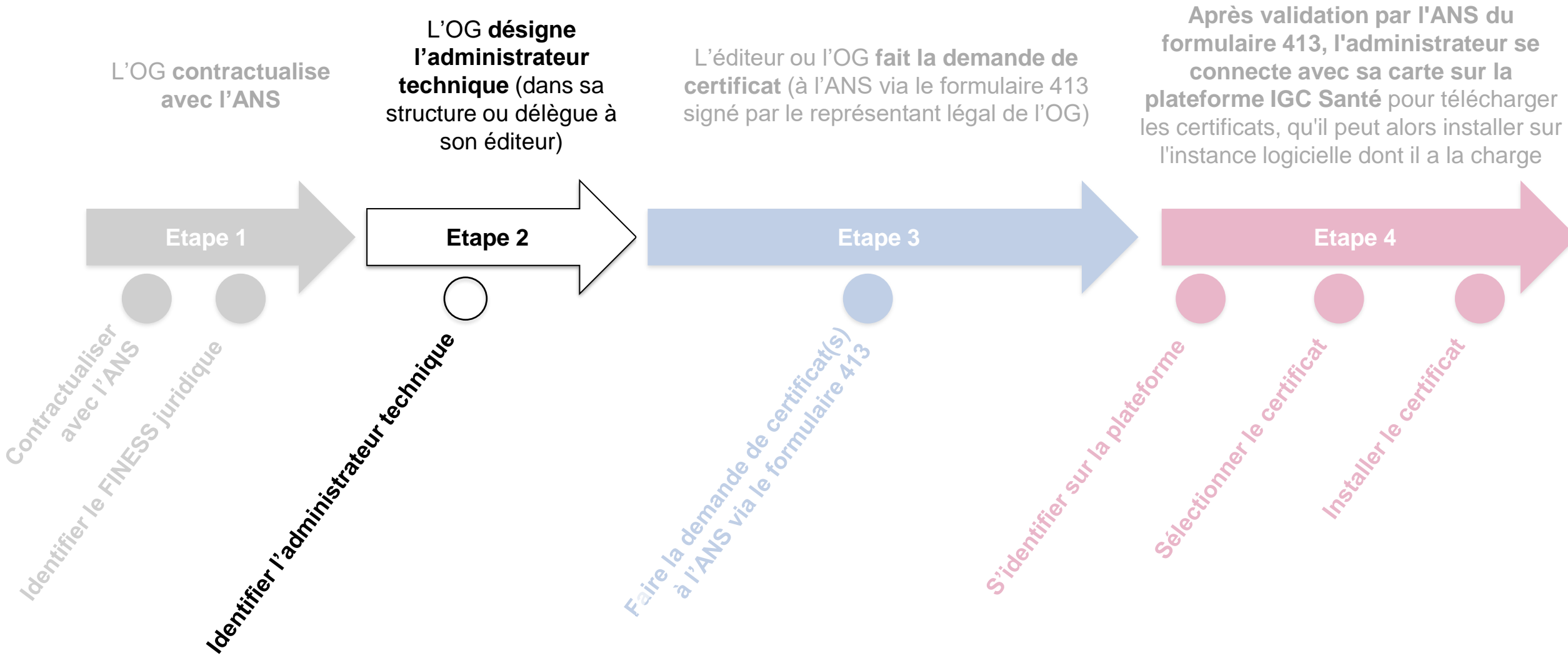
Sélectionner le site dans la liste

Noter le **numéro de FINESS juridique de l'entité juridique de rattachement**

Pour toute question / information nous vous invitons à contacter l'ANS via : [monserviceclient.finess@esante.gouv.fr](mailto:monserviceclient.finess@esante.gouv.fr)

• Démarche d'obtention des certificats : L'OG désigne l'administrateur technique

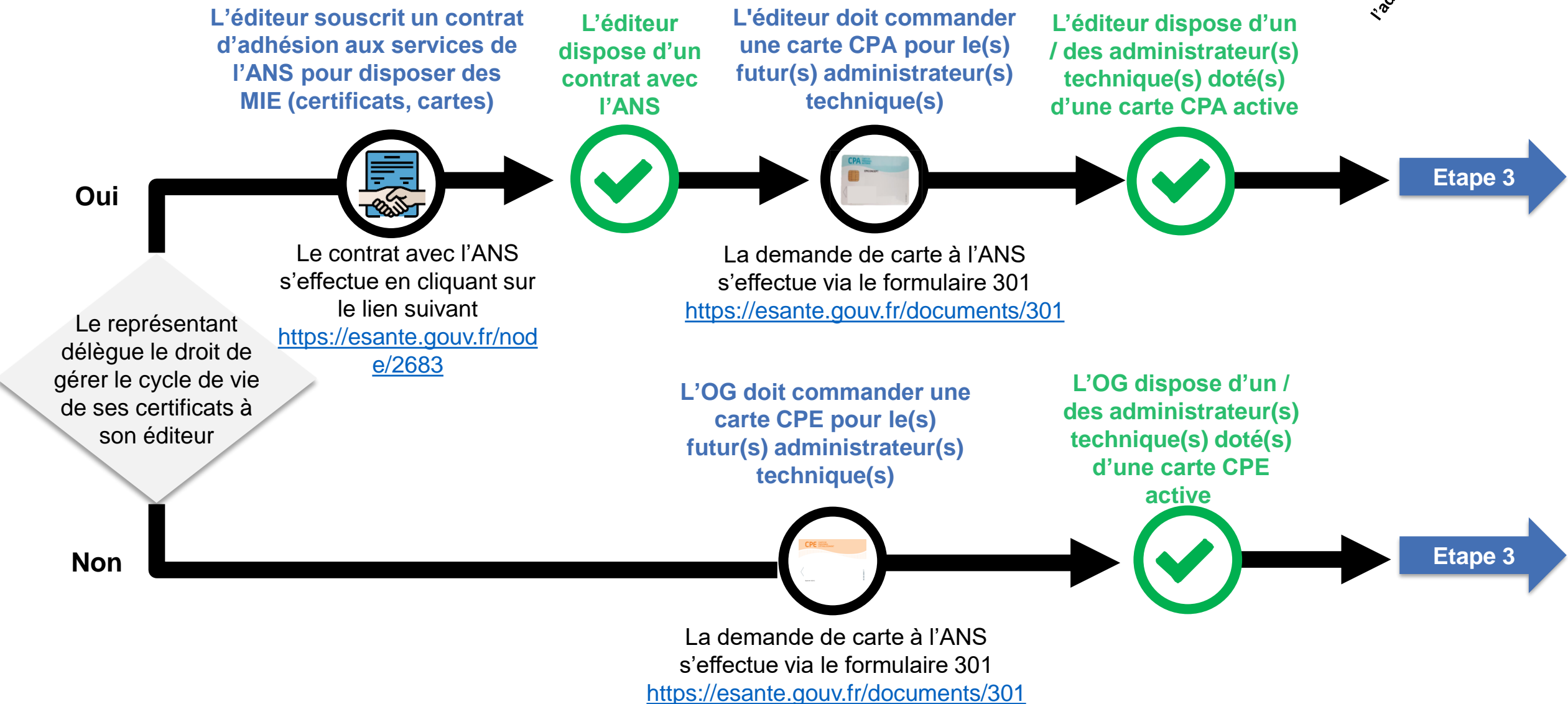
Le schéma ci-dessous présente les différentes étapes nécessaires à l'obtention d'un certificat



• Etape 2 : L'OG désigne l'administrateur technique

Le schéma ci-dessous présente les différentes actions nécessaires à l'étape 2

Identifier l'administrateur technique



## • Etape 2 : Identifier l'administrateur technique



Cliquez pour accéder à la démarche

### Cas 1: L'OG délègue à son éditeur la démarche technique de récupération des certificats

L'éditeur **doit identifier en son sein un ou des administrateur(s) technique(s) et le(s) doter d'une carte valide (CPA).**

**C'est l'administrateur technique de l'éditeur qui se charge de récupérer et d'installer le certificat**



L'aide à l'obtention du certificat logiciel est incluse dans la prestation Ségur



Cliquez pour accéder à la démarche

### Cas 2 : L'OG effectue la récupération des certificats sans délégation à l'éditeur

L'OG **doit identifier en son sein un ou des administrateur(s) technique(s) et le(s) doter d'une carte valide (CPE).**

**C'est l'administrateur technique de l'OG qui se charge de récupérer et d'installer le certificat**



L'installation du certificat nécessite des compétences techniques

La démarche est similaire dans les deux cas, seul le type de carte (CPA pour les éditeurs / CPE pour l'OG) change. Cependant l'éditeur doit auparavant contractualiser avec l'ANS (si aucune contractualisation n'a été réalisée au cours d'autres projets)



## • Etape 2 : Identifier l'administrateur technique

Le représentant légal de l'OG **délègue le droit de gérer le cycle de vie à un ou à des administrateurs techniques** (demande, retrait, révocation et suivi) des certificats logiciels commandés.

S'il est convenu dans le cadre de la contractualisation entre l'OG et l'éditeur que ce dernier prenne en charge la gestion des **certificats de l'OG, l'éditeur doit alors désigner en son sein le ou les administrateur(s) technique(s)**. Un même administrateur technique peut gérer plusieurs certificats pour le compte d'OG différents.

**L'éditeur doit disposer d'un contrat d'adhésion avec l'ANS**



Si l'éditeur ne dispose pas déjà d'un contrat avec l'ANS, il doit contractualiser via le lien ci-dessous : [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/Contrat\\_adhesion.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/Contrat_adhesion.pdf)

**Si un contrat d'adhésion existe déjà** entre l'ANS et l'éditeur (réalisé au cours d'autres projets), il n'est pas nécessaire de re-contractualiser.

**L'éditeur doit commander une carte CPA pour le(s) futur(s) administrateur(s) technique(s)**



Si l'administrateur technique n'a pas encore de carte CPA (Carte de Personnel Autorisé) active, l'éditeur doit compléter une demande d'attribution de carte de personnel de structure via le **formulaire 301** : <https://esante.gouv.fr/documents/301>



**L'éditeur dispose d'un / des administrateur(s) technique(s) doté d'une carte CPA active**

NB : la modification des administrateurs techniques se faire via le **formulaire 503** : [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/F503.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/F503.pdf)



## • Etape 2 : Identifier l'administrateur technique

Le représentant légal de l'OG identifie un ou des **administrateurs techniques** (pour tous les ESSMS de l'OG qui utilisent une même solution de DUI).

L'administrateur technique est la personne qui va procéder à **la génération et au déploiement des certificats utilisés pour la connexion au téléservice INSi / DMP**

**L'OG doit disposer d'un contrat d'adhésion avec l'ANS**

**L'OG doit commander une carte CPE pour le(s) futur(s) administrateur(s) technique(s)**



\* Voir slide 15

Si l'administrateur technique n'a pas encore **de carte CPE** (carte de professionnel d'établissement) active, l'ESSMS doit compléter une demande d'attribution de carte de personnel de structure via le **formulaire 301** :  
<https://esante.gouv.fr/documents/301>

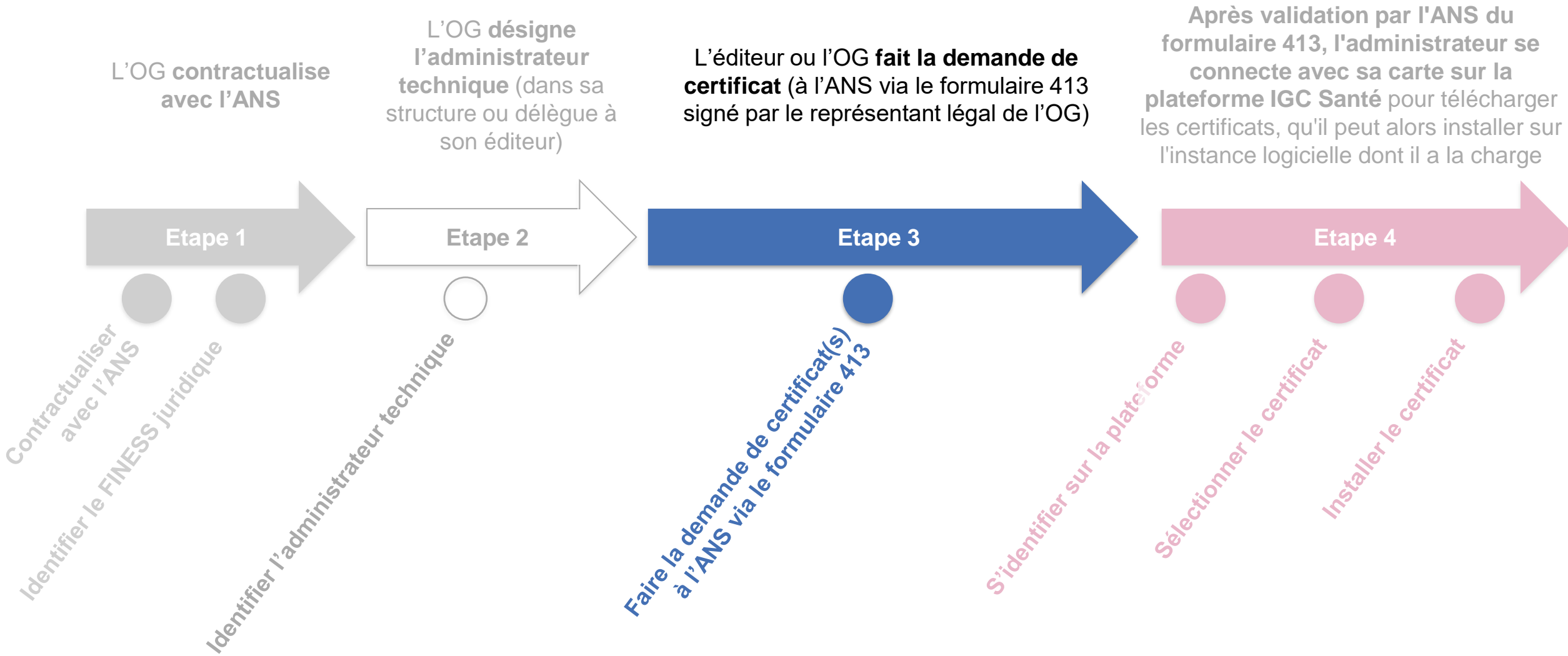


**L'OG dispose d'un / des administrateur(s) technique(s) doté d'une carte CPE active**

NB : la modification des administrateurs techniques se faire via le **formulaire 503** :  
[https://esante.gouv.fr/sites/default/files/media\\_entity/documents/F503.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/F503.pdf)

• **Démarche d'obtention des certificats : la demande de certificat via le formulaire 413**

Le schéma ci-dessous présente les différentes étapes nécessaires à l'obtention d'un certificat





### Etape 3 : L'éditeur ou l'OG fait la demande de certificat

Le schéma ci-dessous présente les différentes actions nécessaires à l'étape 3

Le représentant légal (ou un de ses mandataires) ou l'éditeur renseigne le formulaire 413

Le formulaire est signé par le représentant légal et envoyé à l'ANS

Un mail d'accusé réception, avec un numéro de référence du dossier est transmis dès réception du formulaire

Un mail confirmant la validation de la demande et la possibilité pour l'administrateur technique de se connecter à la plateforme IGC est envoyé au responsable légal et à l'administrateur



Non

Oui



Le support contacte l'administrateur technique et le responsable de la structure en cas d'informations erronées

Ce formulaire est téléchargeable à l'adresse suivante : <https://esante.gouv.fr/documents/413>  
Ou <https://www.demarc-hes-simplifiees.fr/commissariat/413>

Une fois le formulaire complété, l'OG ou l'éditeur le renvoie à l'adresse mail suivante : [monserviceclient.certificats@esante.gouv.fr](mailto:monserviceclient.certificats@esante.gouv.fr)



Cliquez pour accéder au focus du formulaire 413

• **Etape 3 : Faire la demande de certificat(s) à l'ANS via le formulaire 413**

**Le formulaire 413 doit être complété par l'éditeur / OG et être signé par le représentant légal de l'OG**

Ce formulaire est téléchargeable à l'adresse suivante : <https://esante.gouv.fr/documents/413> ou sur <https://www.demarches-simplifiees.fr/commencer/f413>

**Le représentant légal (ou un de ses mandataires) ou l'éditeur renseigne le formulaire 413 :**

**Le représentant légal (ou un de ses mandataires) ou l'éditeur envoie le formulaire 413 :**

**Le support ANS informe la structure de l'état d'avancement de sa demande :**



Le représentant légal ou l'éditeur déclare un ou plusieurs administrateurs techniques autorisés à gérer les certificats logiciels et précise les types de certificats souhaités

**Un guide détaillant les informations à renseigner dans le formulaire 413 est disponible en annexe** en cliquant sur l'icône



*Cliquez pour accéder au focus du formulaire 413*

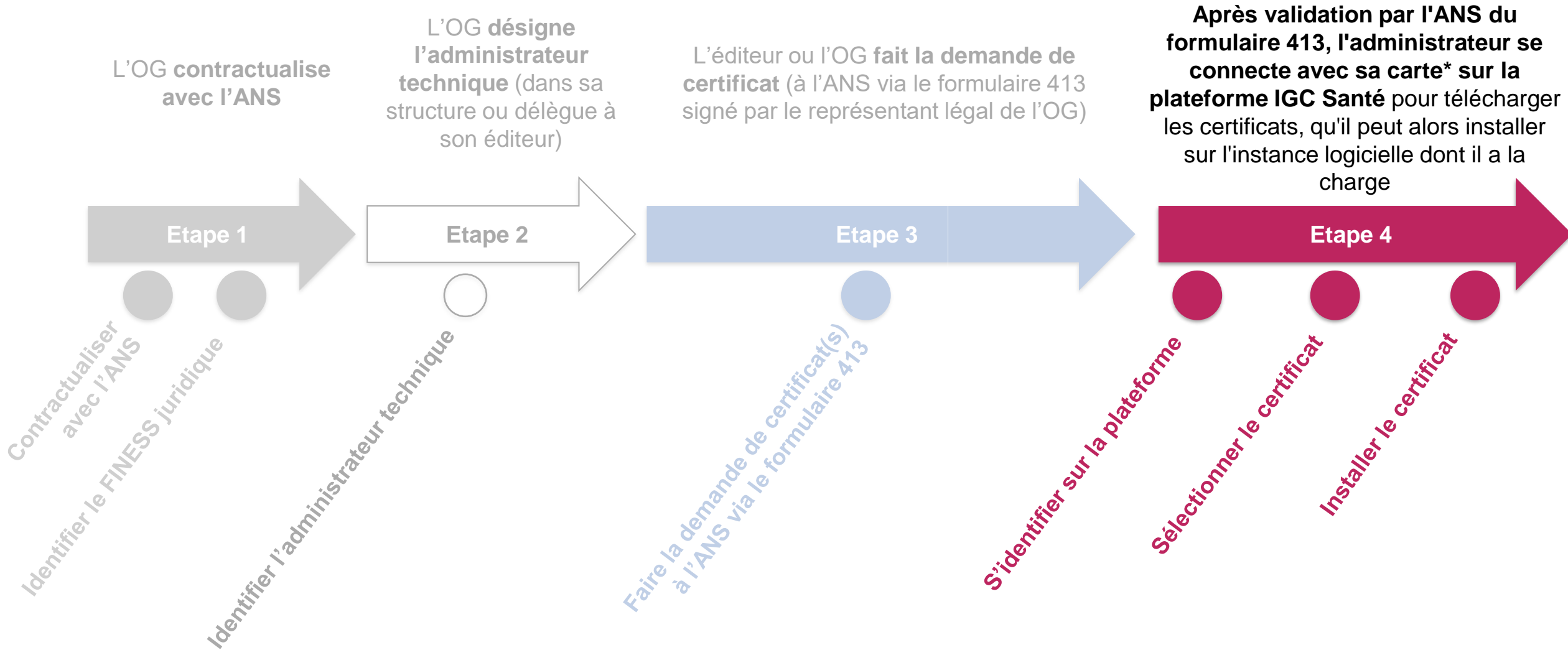
Une fois le formulaire complété et signé par le représentant légal, l'éditeur le renvoie à l'adresse mail suivante : [monserviceclient.certificats@esante.gouv.fr](mailto:monserviceclient.certificats@esante.gouv.fr) et **reçoit un message d'accusé réception, avec un numéro de référence du dossier.**

Le responsable de la structure indiquée dans le formulaire 413 et l'administrateur **technique seront informés par mail du traitement de la déclaration d'habilitation à commander des certificats.** Cette démarche prend environ 3 jours ouvrés. Le support vous contacte en cas de difficulté.

**Un mail de confirmation de la validation de la demande vous permet de savoir quand l'administrateur peut ensuite aller se connecter et télécharger les certificats.**

• **Démarche d'obtention des certificats : l'administrateur technique récupère les certificats**

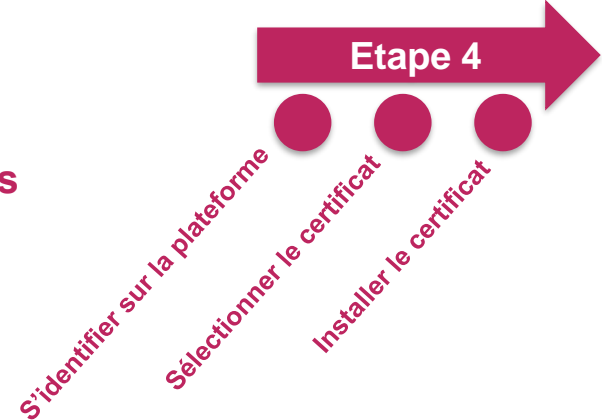
Le schéma ci-dessous présente les différentes étapes nécessaires à l'obtention d'un certificat



\* Il faut pour cela se doter d'un lecteur de carte

● **Etape 4 : L'administrateur technique récupère les certificats**

Le schéma ci-dessous présente les différentes actions nécessaires à l'étape 4



**L'administrateur technique autorisé se connecte sur la plateforme IGC Santé avec sa carte CPA / CPE**



**L'administrateur technique sélectionne les certificats avec un identifiant FINESS juridique**



**L'administrateur technique télécharge les certificats (et s'il y a 2 instances, il télécharge 2 certificats avec le même identifiant FINESS)**



**L'administrateur technique installe les certificats sur son instance logicielle**



**L'installation des certificats est réalisée. Les services numériques peuvent être utilisés**



L'administrateur technique peut récupérer ses certificats en se connectant sur la plateforme IGC Santé à l'adresse suivante : <https://pfc.eservices.esante.gouv.fr>

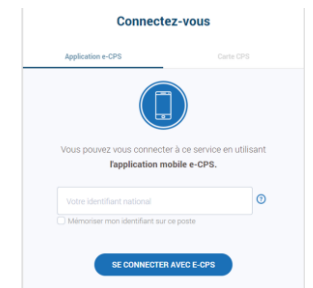
● **Etape 4 : Implémenter le(s) certificat(s) : S'identifier sur la plateforme**

A réception du mail de validation de la commande des certificats, l'administrateur technique (éditeur / OG) **habilité peut récupérer** ses certificats en se connectant sur la plateforme IGC Santé à l'adresse suivante : <https://pfc.eservices.esante.gouv.fr>. L'administrateur technique dispose de deux options pour se connecter :

**Se connecter via sa carte CPX (carte CPE / CPA) au téléservice de commande.** Le poste de travail utilisé doit alors être équipé d'un lecteur de carte à puce.



**Se connecter via sa eCPx (à activer auparavant par la carte CPx) pour se connecter au téléservice de commande.**



● **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

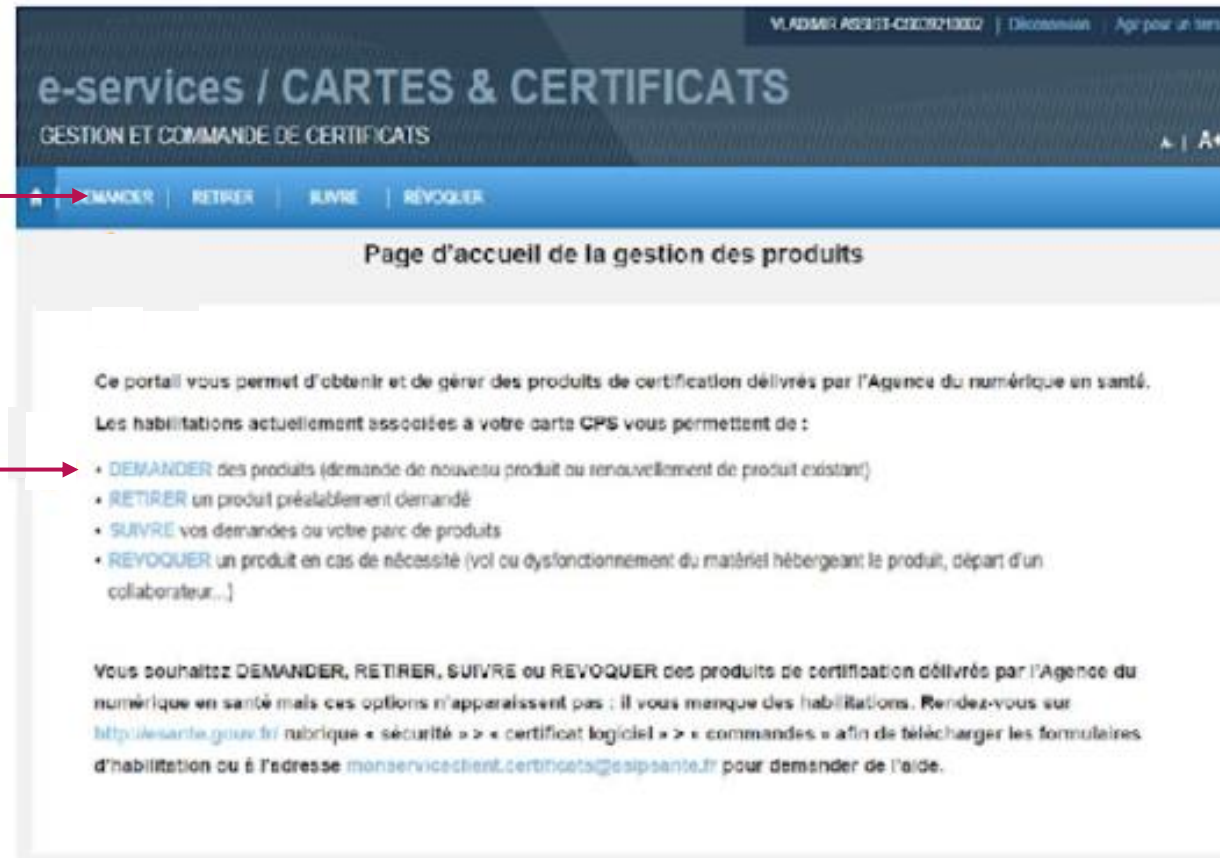
L'administrateur technique **peut accéder aux processus de récupération de certificat de deux manières :**

**Cliquer sur l'onglet en haut à gauche**



OU

**Cliquer sur le menu de gestion des produits**



• **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

L'administrateur technique sélectionne le type d'offre et sa structure :

**Sélectionner « ORG »** (les autres types de certificats ne sont pas pertinents pour ce guide).

**Rechercher et sélectionner la structure adéquate.**

**Cliquer sur Suivant (à faire pour chaque étape)**

● **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

Une fois l'offre, la structure et le bénéficiaire identifiés, l'administrateur technique peut réaliser la demande pour le nouveau certificat.

Pour créer un nouveau certificat, cliquez sur « Demander un nouveau produit »

**Demande de produit**

Etape 1
Etape 2
Etape 3
Etape 4
Finalisation

DEMANDER UN NOUVEAU PRODUIT

Si vous ne souhaitez pas demander un nouveau produit, choisissez dans la liste qui suit le produit que vous souhaitez renouveler.

N° produit	Canal	Offre	Usage	Bénéficiaire	Service applicatif	Adresse mail	Demandeur	Etat
Pas de résultat								

ANNULER
PRÉCÉDENT

Pour renouveler un certificat déjà existant, cliquez sur la « flèche » à droite de la mention « Recherche » pour afficher les certificats logiciels existants à renouveler.



● **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

L'administrateur technique précise l'ensemble des informations nécessaires à la création de la demande.

**e-services / CARTES & CERTIFICATS**  
GESTION ET COMMANDE DE CERTIFICATS

EN LANCER | HISTOIRE | SERVICES | RÉGULIER

**Demande de produit**

Etape 1 | Etape 2 | **Etape 3** | Etape 4 | Finalisation

Récapitulatif des informations renseignées

Site:   
Statut:

Usages

Usage	Description
AUTH, CLI	Authentification Client
CONF	Chiffrement
SIGN	Signature Digitale

Informations de produit

\*Service exploit:

Informations de contact

\*Email de l'acteur:  @

Email d'une personne à informer:  @

ANNULER | DÉTAILS DU PRODUIT | PRÉCÉDENT | SUIVANT

Dans l'encart « Récapitulatif »,  
les informations sont  
automatiquement  
renseignées

« Informations de produit »  
(voir slide suivante – **slide 31**)

« Informations de contact »  
(voir **slide 32**)

• **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

L'encart « Informations de produit » est à renseigner, son contenu, qui sera ainsi retrouvé dans le champ 'CN=' du certificat, est adapté en fonction de l'usage sélectionné (certificat INSi ou hors INSi) :

A l'exception de l'INSi, ce champ libre désigne **une application** ou **une structure** (Exemples : « SAMU 75 », « Proxy DMP CHU Nantes »)

**Règles de commande particulières pour les certificats INSi**



Veillez saisir dans la zone **Service applicatif** :

- la valeur **INSI-AUTO** pour les usages de type « automatisés » / « batch »
- la valeur **INSI-MANU** pour les usages de type « manuels »

**Attention à bien respecter les majuscules et à ne pas rajouter d'espaces**



Vous trouverez ci-dessous le guide détaillant les spécificités du service INSi : [https://www.sesam-vitale.fr/documents/20182/75606/SEL-MP-043\\_01-00\\_INSi+sans+MR](https://www.sesam-vitale.fr/documents/20182/75606/SEL-MP-043_01-00_INSi+sans+MR), et notamment son annexe 3

• **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

L'encart « Informations de contact » permet d'indiquer les destinataires des notifications des actions réalisées ou à réaliser

**Renseigner obligatoirement**  
« Email de l'acteur »

**Renseigner de manière facultative**  
« l'email d'une personne à informer »

- « **Email de l'acteur** », concerne la personne qui fait la demande c'est-à-dire l'administrateur technique habilité. Ce champ est **obligatoire**. Il permet de recevoir les notifications par email des actions réalisées ou à réaliser (confirmation de la demande, mise à disposition du certificat...). Attention ce champ n'est pas récupéré automatiquement via le formulaire 413, il faut le renseigner à nouveau.
- « **L'email d'une personne à informer** », élément **facultatif** à renseigner. Cette adresse est utilisée pour envoyer des notifications à titre informatif sur les actions réalisées (confirmation de la demande, mise à disposition du certificat...). Ce champ est équivalent à un champ 'CC / copie conforme'.

● **Etape 4 : Implémenter le(s) certificat(s) : Sélectionner le certificat**

La CSR (Certificate Signing Request = demande de signature de certificat) est nécessaire pour obtenir un certificat. Elle doit être créée sur le serveur sur lequel le certificat sera installé et contient des informations que l'autorité de certification (AC) utilisera pour créer le certificat. La CSR contient également la clé publique qui sera incluse dans le certificat. La clé privée correspondante n'est pas incluse dans la CSR, mais est utilisée pour signer numériquement la demande.

L'administrateur technique doit fournir un fichier CSR pour finaliser la demande, avec deux cas possibles :

- **Cas 1 : Soit l'administrateur technique dispose déjà d'une CSR et il la télécharge sur la plateforme.**
- **Cas 2 : Soit l'administrateur technique n'a pas de CSR et peut la créer en ligne.** Cette option permet de créer la CSR en ligne de manière assistée. Elle évite de devoir construire une CSR.

**Cas 1**  
Pour charger une CSR, cliquer sur « Charger la CSR ».

**Cas 2**  
Pour créer la CSR en ligne, cocher la case correspondante.

- **Etape 4 : Implémenter le(s) certificat(s) : Installer le certificat**



Demande de produit

Etape 1    Etape 2    Etape 3    Etape 4    Finalisation

Votre demande a été prise en compte.  
Vous allez recevoir un email de confirmation.

+ DEMANDER UN AUTRE PRODUIT  
✓ TERMINER

**Cliquer sur** « Terminer »  
en bas à droite pour  
clôturer la procédure

L'administrateur technique reçoit des notifications par email pour l'informer de l'avancement de la demande de Certificat Logiciel. Il pourra ensuite installer le certificat logiciel.

L'installation du certificat est dépendante de l'implémentation de chaque logiciel (magasin de certificat propre au logiciel, magasin windows...). L'administrateur technique devra donc se rapprocher de l'éditeur pour finaliser l'installation.

**Le certificat délivré par l'ANS a une durée de validité de 3 ans à compter de son obtention. Une notification est envoyée un mois avant l'expiration du certificat à l'adresse mail / aux adresses mails de(s) administrateur(s) technique(s) renseignées sur la plateforme.** Par sécurité, nous vous recommandons d'implémenter une alerte du côté de l'administrateur pour penser aux renouvellements.

En cas de changement d'administrateur technique (départ / arrivée / etc.), l'éditeur peut faire les changements via le formulaire 503 : [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/F503.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/F503.pdf)



**Nous vous invitons à renouveler le certificat avant la date d'expiration, sous peine de rupture de service pour les utilisateurs.**

• **Etape 4 : Implémenter le(s) certificat(s) : les bonnes pratiques**



**Ne pas dupliquer le certificat et la clé privée**

Un même certificat et sa clé privée peuvent être utilisés pour s'authentifier sur plusieurs services numériques en santé depuis la même instance logicielle (ou le même serveur) mais le certificat et la clé privée ne doivent pas être dupliqués.

Si l'accès à un ou plusieurs services est réalisé depuis des instances logicielles (ou des serveurs) différents alors **il faut générer 2 certificats différents et 2 clés privées différentes**. Dans ce cas, ils peuvent porter le même identifiant FINESS ou des identifiants FINESS différents, pour mieux distinguer les usages respectifs.



**Ne pas envoyer la CSR par mail**

La CSR, qu'elle soit générée sur la plateforme IGC Santé ou fournie par l'administrateur, est sensible.

**En cas de transmission nécessaire de ce document, il faut veiller à la sécurisation de son envoi, par exemple avec une plateforme sécurisée (ex: conteneur Zed, etc.) et l'envoi du mot de passe sur un canal séparé.**

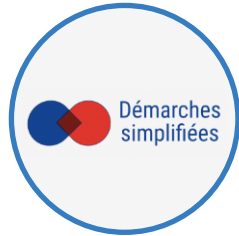


Vous trouverez ci-dessous la FAQ relative à la plateforme IGC  
<https://industriels.esante.gouv.fr/faq-des-industriels?f%5B0%5D=theme%3A624>

# Futures évolutions



Différentes évolutions sont à l'étude afin de **faciliter le déploiement des certificats** tout en garantissant **la sécurisation des informations et des processus** :



Permettre **une démarche en ligne complète** pour les éditeurs et les structures de santé (sanitaire, médico-social et social)

**Eviter l'impression des formulaires**



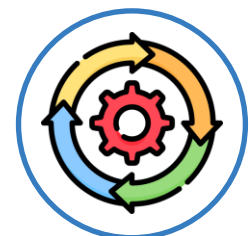
Permettre l'**habilitation en masse d'un administrateur technique d'un éditeur** ayant une volumétrie de clients importante

**Eviter la multiplication des formulaires 413**



**Gérer les habilitations des administrateurs techniques par l'éditeur** et non par la structure cliente délégataire

**Anticiper le "turn over" des administrateurs techniques**



**Autoriser le renouvellement automatique** des certificats

**Faciliter la continuité du service**



# Annexes



## Faire la demande de certificat(s) à l'ANS via le formulaire 413 : indiquer les informations relatives à la structure et au représentant légal

Compléter la partie 3.1 (Identification de la structure) et 3.2 (Identification du représentant légal ou du mandataire) en renseignant les informations suivantes :

3. Identification de la structure bénéficiaire <i>(L'ensemble des champs doit être complété)</i>												
3.1 Identification de la structure												
Dénomination de la structure												
FINESS * voir notice ci-jointe (uniquement pour les structures prenant en charge des patients / usagers)												
<b>ou</b> N° SIRET												
RPPS rang <sup>(1)</sup> (uniquement pour les cabinets de radiologie, hors sociétés d'exercice)	1.											
	2.											
	3.											
	4.											

Dénomination de la structure, c'est-à-dire la **raison sociale de l'OG**

Numéro de **FINESS** juridique de l'OG

Ne pas remplir

Ne pas remplir

3.2 Identification du représentant légal ou du mandataire ou titulaire du cabinet <i>(uniquement pour les RPPS Rang)</i>												
Êtes-vous le :	<input checked="" type="radio"/> Responsable légal <input type="radio"/> Mandataire <input type="radio"/> Titulaire du cabinet											
Nom												
Prénom(s)												
Téléphone												
Email professionnel												
N° de carte												

Cocher la case « responsable légal »

Indiquer l'identification et les coordonnées du responsable légal de l'OG

*Bonnes pratiques : le certificat étant à renouveler tous les 3 ans, il peut être pertinent de renseigner une adresse générique afin d'anticiper le turn over*

## Faire la demande à l'ANS via le formulaire 413 : Indiquer les informations relatives à la structure et au représentant légal

Indiquer les coordonnées des ressources de l'éditeur ou de l'OG ayant un rôle d'administrateur technique.

4. Informations spécifiques				
4.1 Déclaration des administrateurs techniques				
N° de carte *	Nom figurant sur la carte *	Prénom figurant sur la carte *	Téléphone *	Email professionnel *

Indiquer le numéro de carte (3<sup>ème</sup> ligne de la carte, numéro à 10 chiffres), les coordonnées **de l'administrateur ou des administrateurs techniques de l'éditeur ou de l'OG**

*Bonnes pratiques : le certificat étant à renouveler tous les 3 ans, il peut être pertinent de renseigner une adresse générique afin d'anticiper le turn over*

Pour toute information sur le numéro de carte, veuillez consulter le document ci-dessous:  
[https://esante.gouv.fr/sites/default/files/media\\_entity/documents/CGU\\_Produits\\_Certification\\_2.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/CGU_Produits_Certification_2.pdf)

4.2 Usage des certificats et solution utilisée	
Précisions sur l'usage des certificats et sur votre projet *	
Éditeur de la solution	
Solution utilisée	

← Ne pas remplir

← Indiquer le nom de l'éditeur

← Indiquer le nom de la solution utilisée

- Faire la demande à l'ANS via le formulaire 413 : Indiquer le type de certificat

**4.3 Type de certificats souhaités**  
Cochez les types de certificats souhaités et remplissez les informations complémentaires associées

<input checked="" type="checkbox"/>	<b>Certificat ORG (Personne morale) usage AUTH_CLI, SIGN, CONF (Ex : DMP, ROR, Annuaire Santé...)</b>
<input type="checkbox"/>	<b>Certificat logiciel SERVEUR usage SSL_SERVEUR (Ex : MSSanté, Diapason, PSIG...)</b> <i>Remplir l'une des lignes suivantes :</i>
Certificat pour le nom de domaine suivant : (Veuillez indiquer le nom de domaine souhaité / adresse web, ex : domaine.fr.)	
<b>OU</b> Certificat restreint au serveur suivant : (Veuillez indiquer le nom de serveur spécifique, ex : nomdeserveur.domaine.fr)	
<input type="checkbox"/>	<b>Certificat logiciel SERVEUR usage SMIME, SIGN, CONF (Ex : Messagerie HPRIM NET...)</b> <i>Remplir la ligne suivante :</i>
Certificat pour le nom de domaine de messagerie suivant : (Veuillez indiquer uniquement le nom de domaine souhaité, ex : @domaine.fr.)	
<input type="checkbox"/>	<b>Certificat logiciel PRO (Personne physique) usage AUTH, SIGN, CONF (Ex : Dossier Pharmaceutique...)</b> <i>Remplir la ligne suivante :</i>
Certificat pour le nom de domaine de messagerie suivant : (Veuillez indiquer uniquement le nom de domaine souhaité, ex : @domaine.fr.)	

← Cocher la case « **offre certificat logiciel ORG (personne morale) usage AUTH\_CLI, SIGN, CONF pour disposer des certificats DMP et INSI** »



**esante.gouv.fr**

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

**tech.esante.gouv.fr**

Le portail dédié aux Industriels.

 **@esante\_gouv\_fr**

 **linkedin.com/company/agence-du-numerique-en-sante**