

Annexe 2.3 : CCTP - Authentification unique pour les applications web

-

Dossier client de définition du service

Fiche de contrôle du document

Historique des versions

Version	Date	Rédacteur	Modification
0.6	12/11/10		Correction après réunion du 10/11 + quelques corrections sur les parties de Thierry + ajout apports + qualité de
0.7	22/11/10	Thierry Delprat	Corrections / apports
0.81	15/01/2011	M4	Séparation des parties fournisseur / client
0.82	21/01/2011	M4	Prise en compte des remarques, intégration des processus « client »
1.0	04/02/2011	M4	Passage en version finale
1.1	14/03/2011	M4	Modification du chapitre 3.3.3

Processus de validation

Rédacteur		Date de rédaction	
Approbateur		Date d'approbation	
Valideur		Date de validation	

Sommaire

1. Glossaire	5
2. Objet du dossier de définition du service	5
3. Contenu du service	6
3.1. Objet du service	6
3.2. Types de service	6
3.2.1. Type « SSO basique »	6
3.2.2. Type « SSO avancé »	6
3.2.3. Type « SSO étendu »	8
3.3. Périmètre d'application du service	10
3.3.1. Périmètre « utilisateurs »	10
3.3.2. Périmètre « applications »	10
3.3.3. Matrice de décision	11
3.3.4. Exemples d'usage	11
3.4. Apports du service	12
3.4.1. Pour les utilisateurs	12
3.4.2. Pour les gestionnaires d'application	12
3.5. Périodes de service et qualité de service	13
3.5.1. Pour les incidents	13
3.5.2. Pour les changements	13
3.5.3. Pour les demandes initiales de raccordement ou de modification	14
4. Solutions disponibles et critères d'éligibilité au raccordement	15
4.1. Aperçu des solutions disponibles	15
4.2. Critères d'éligibilité au raccordement pour les applications	15
4.2.1. Pré-requis généraux au raccordement pour les applications	15
4.2.2. Critères spécifiques au type de service « SSO avancé »	16
4.2.3. Critères spécifiques au type de service « SSO étendu »	16
4.3. Principes de délégation de l'authentification	16
4.3.1. Principes communs aux solutions techniques	16
4.3.2. Principes SSO Basique	16
4.3.3. Principes SSO Avancé	16
4.3.4. Principes SSO Étendu	17
5. Contacts et rôles	18
5.1. Contacts clients	18
5.2. Contacts fournisseur	18

6. Processus de livraison et de gestion du service	19
6.1. Processus de traitement d'une demande initiale ou de modification	19
6.2. Processus de gestion des incidents	21
6.3. Processus de gestion des évolutions et des changements.....	23
6.3.1. Évolutions.....	24
6.3.2. Changements majeurs	25
6.3.3. Changements mineurs	28
7. Indicateurs	30
8. Annexes.....	31
8.1. Schéma des composants techniques pour le type de service « SSO basique »	31
8.2. Schéma des composants techniques pour le type de service « SSO avancé »	31
8.3. Schéma des composants techniques pour le type de service « SSO étendu »	32

1. Glossaire

Terme	Signification
Agent externe déclaré dans l'annuaire Ldap	Utilisateur non INRAE déclaré dans le référentiel d'authentification de l'institut et qui n'est pas renseigné dans le référentiel agent Inra (S2IRH)
Annuaire LDAP	Annuaire d'entreprise utilisant le protocole LDAP (Lightweight Directory Access Protocol)
Attribut LDAP	Caractéristique d'une fiche utilisateur au sein du référentiel d'authentification d'INRAE (Service LDAP) : exemple Nom, Prénom, Mail...
Gestionnaire d'application	Responsable / représentant de l'application au sein d'INRAE
Heures ouvrées	9h-17h
Identification	Connaître l'identité de l'utilisateur
Jours ouvrés	Du lundi au vendredi, sauf jours fériés.
Référent technique	Interlocuteur technique privilégié sur la gestion de l'authentification au sein de l'application souhaitant se raccorder
Référentiel Agent INRAE	S2IRH : référentiel garant des informations sur les agents travaillant pour INRAE.
WEBSSo	Mécanismes d'authentification unique pour les applications WEB

2. Objet du dossier de définition du service

Ce document a pour objectif de présenter le cadre du service « Authentification unique pour les applications web », que la DSI propose pour faciliter la navigation des utilisateurs finaux sur les applications du SI accessibles via une interface web.

Ce dossier est le document de référence que se partagent le fournisseur (la DSI) et les clients du service. Il définit son périmètre d'utilisation en termes d'applications et de populations éligibles, détaille les différents types de services et solutions techniques mises à disposition, décrit de façon exhaustive l'ensemble des processus de livraison et de gestion du service, les conditions d'utilisation du service et les responsabilités de l'ensemble des acteurs.

Les éléments contractuels issus de ce document (engagements des deux parties, qualité de service, contacts, etc.) sont intégrés dans un contrat de service, qui sera signé par le Client et le Fournisseur. Le contrat de service fait référence à ce document.

3. Contenu du service

3.1. Objet du service

L'objet principal du service est de faciliter la navigation sur les sites web et sur les applications métiers d'INRAE accessibles depuis une interface web, en permettant aux utilisateurs de ne procéder qu'à une seule saisie de leur login/mot de passe.

Les solutions techniques mises en œuvre pour ce service s'appuient sur le référentiel d'authentification d'INRAE. Elles peuvent être élargies aux référentiels d'organismes partenaires pour permettre à leurs utilisateurs d'accéder aux applications qu'INRAE mettra à leur disposition.

Le service offre également la possibilité d'enrichir les profils utilisateurs dans les applications clientes. Cette fonctionnalité est rendue au travers de la fourniture d'attributs (voir liste des attributs disponibles dans le paragraphe 3.2.3) aux applications clientes qui le souhaitent.

Enfin, ce service augmente la sécurité de la phase d'authentification en limitant la diffusion du login/mot de passe.

3.2. Types de service

Le service « Authentification unique pour les applications web » se décline en trois types de service pour répondre à l'ensemble des besoins.

3.2.1. Type « SSO basique »

Fonctionnalités :

- Délégation de l'authentification de l'application cliente au service d'authentification (WEBSSO) auprès du référentiel d'authentification (Annuaire Ldap) qui contient les agents INRAE et des utilisateurs externes.
- Sécurisation de l'authentification des applications raccordées.
- L'application peut récupérer l'identifiant saisi par l'utilisateur afin de gérer des rôles elle-même.

3.2.2. Type « SSO avancé »

Fonctionnalités :

- Mêmes fonctionnalités que le type « SSO basique »
- Habilitation de l'accès à la ressource : l'habilitation est réalisée par le service authentification unique et non par l'application. Cette habilitation repose sur un contrôle réalisé via des attributs parmi la liste suivante disponible dans l'annuaire Ldap :

Attribut Ldap	Valeur	Description	Périmètre d'application	Exemple
Appli	INTRA_UTILI	Droit d'accès à l'intranet INRAE	Droit d'accès à l'intranet INRAE	appli = INTRA_UTILI
Appli	Chaîne de caractère (maximum 10 caractères)	Identifie de manière unique un projet	Donne le droit d'accès à une application pour les agents déclarés en tant qu'externe dans le cadre d'un projet identifié	appli = MONAPPLI_UTILI
CentrePrincipal	2 chiffres	Code du centre de rattachement des agents	Permet de filtrer sur le centre de rattachement des agents	centrePrincipal = 13
Centre	2 chiffres	Code du ou des centres sur lesquels les agents sont autorisés à travailler	Permet de filtrer sur les centres sur lesquels les agents sont autorisés à travailler	centre = 11
Unite	4 chiffres maximum	Codes unités dans lesquelles travaillent les agents	Permet de filtrer sur unités des agents	unite = 1022
DepartmentNumber	2 chiffres	Codes de départements de recherche auxquels sont	Permet de filtrer sur les départements de recherche	departmentNumber = 60
Direction	Chaîne de caractères	Acronyme de directions auxquels sont	Permet de filtrer sur les directions d'appui à la recherche	Direction = DSI
Role1	Chaîne de caractère. Valeurs possibles : CD, CDADJ, DAR, DARADJ, DARD, DASA, DELREJ, DGDA, DS,	Acronyme de mandats de agents.	Permet de filtrer sur les mandats des agents	Role1 = DU

	DSA, DSAADJ, D U, DUADJ, PC, P CADJ, PRES, R M, VPNE			
--	---	--	--	--

Remarque : ce type de service est soumis à des critères d'éligibilité particuliers. (§4.2.2)

3.2.3. Type « SSO étendu »

Fonctionnalités :

- Mêmes fonctionnalités que le type « SSO basique »
- Utilisation des référentiels agents de nos partenaires pour la phase d'authentification (la liste des partenaires éligibles est disponible à cette adresse : <https://federation.renater.fr/participants/idp>)
- Fourniture d'attributs à l'application cliente, ce qui permet à celle-ci une gestion fine des rôles applicatifs. Cette gestion des rôles reste à la charge de l'application. Les attributs fournis par le service sont les suivants :

Attributs fournis	Valeur	Description	Périmètre d'application	Exemple
Affiliation	member@inrae.fr	Dérivé de la valeur INTRA_UTILI de l'attribut appli de l'annuaire LDAP appartenance à l'institut pour la fédération	Ensemble des applications enregistrées dans la fédération Éducation-recherche	member@inrae.fr
Common name (cn)	<Prénom> <Nom>	Fourni par l'annuaire LDAP Prénom Nom	Ensemble des applications enregistrées dans la fédération Éducation-recherche	Sarah Leprat
Entitlement	urn:mace:dir:entitlement:common-lib-terms	Dérivé de la valeur REVUE_UTILI de l'attribut appli de l'annuaire LDAP Estampille qui peut donner le droit d'accès aux revues électroniques	Utilisé au sein de la Fédération Éducation-recherche pour les revues électroniques	urn:mace:dir:entitlement:common-lib-terms

eduPersonPrincipalName (eppn)	<uid>@inrae.fr	Construit du login de l'utilisateur concaténé de «@inrae.fr». Cet attribut permet d'identifier l'utilisateur dans son institut de rattachement Identifiant unique au sein de la fédération	Ensemble des applications enregistrées dans la fédération Éducation-recherche	sleprat@inrae.fr
Mail	<adresse de message>	Attribut mail de l'annuaire LDAP Adresse mail de l'agent	Ensemble des applications enregistrées dans la fédération Éducation-recherche	Sarah.leprat@toulouse.inrae.fr
Persistent-id	<URL fournisseur d'identité> !<URL fournisseur de service> ! empreinte du login de l'utilisateur	Identifiant opaque de l'utilisateur pour la ressource Identifiant unique anonymisé	Ensemble des applications enregistrées dans la fédération Éducation-recherche	https://idp.inra.fr/idp/shibboleth!https://services-federation.renater.fr/validation/ressource!ZjS0gtJYGjKdK5YVD5M+1FF2
Primary-orgunit-dn	<code centre de rattachement>	Attribut centrePrincipal de l'annuaire LDAP Code centre de rattachement	Ensemble des applications enregistrées dans la fédération Éducation-recherche	14
uid	<login utilisateur>	Attribut uid (login) de l'annuaire LDAP Identifiant de connexion	Ensemble des applications enregistrées dans la fédération Éducation-recherche	sleprat
Unscoped-affiliation	member	Dérivé de la valeur INTRA_UTIL de l'attribut appli de l'annuaire LDAP identifie l'appartenance à la fédération	Ensemble des applications enregistrées dans la fédération Éducation-recherche	member
EmployeeNumber	<employeeNumber>	Attribut employeeNumber de l'annuaire LDAP Matricule de l'agent	Soumis à validation du responsable du service (utilisation limitée)	45738N

Remarque : ce type de service s'appuie sur la solution de fédération d'identité Éducation-Recherche développée par Renater. Une description des attributs utilisables au sein de la fédération Éducation-Recherche est consultable à l'URL suivante :

<https://federation.renater.fr/technique/attributs>.

3.3. Périmètre d'application du service

3.3.1. Périmètre « utilisateurs »

Le service est disponible aujourd'hui pour deux types de population :

- Les utilisateurs enregistrés dans le référentiel d'authentification INRAE.
- Les utilisateurs des établissements d'enseignement supérieur et de la Recherche inscrits au sein de la fédération d'identité Éducation-Recherche.

Remarque : les personnes non INRAE, hors fédération d'identité Éducation-Recherche et non renseignées dans notre référentiel d'authentification ne peuvent bénéficier du service. Il existe toutefois des possibilités de les renseigner dans notre référentiel. Pour plus de précisions, le service à contacter est ldapmaster@inrae.fr.

3.3.2. Périmètre « applications »

Le service est proposé à l'ensemble des sites web et applications métiers d'INRAE accessibles depuis une interface web. Le service s'adresse aux applications nouvelles ou déjà en phase de production.

Remarque : les applications hébergées à l'extérieur d'INRAE sont également autorisées à bénéficier de ce service.

3.3.3. Matrice de décision

La matrice de décision ci-dessous permet pour une application de déterminer le type de service adapté en fonction du besoin d'authentification et d'identification d'une part, et du périmètre de population souhaité d'autre part.

Périmètre utilisateurs / besoin d'authentification et d'identification	Utilisateurs présents dans les référentiels INRAE	Utilisateurs présents dans les référentiels Inra + Utilisateurs de la communauté Éducation-Recherche	Utilisateurs présents dans les référentiels Inra + Utilisateurs hors communauté Éducation-Recherche
Authentification simple	SSO basique	SSO étendu	<i>Non disponible*</i>
Authentification avec habilitation des accès (attributs présentés ci-dessus)	SSO avancé	<i>Non disponible</i>	<i>Non disponible*</i>
Authentification avec fourniture d'attributs (attributs présentés ci-dessus)	SSO étendu	SSO étendu	<i>Non disponible*</i>

* : Lorsqu'un utilisateur non présent dans les référentiels INRAE ou dans la communauté Éducation-Recherche a besoin d'accéder à une application utilisant le service d'authentification unique, il peut faire une demande auprès de son gestionnaire d'application, afin que celui-ci fasse créer un compte dans l'annuaire Inra approprié.

Remarque : Les applications doivent également répondre aux critères d'éligibilité (voir paragraphe 4.2).

3.3.4. Exemples d'usage

- **SSO basique** : application scientifique sur un centre dont les utilisateurs sont uniquement INRAE ;

- **SSO avancé** : site web existant sur l'intranet INRAE hébergé à Jouy-en-Josas souhaitant se raccorder au service d'authentification unique pour ses utilisateurs ;
- **SSO étendu** : application ouverte à nos partenaires et/ou souhaitant récupérer des attributs utilisateurs des référentiels.

3.4. Apports du service

3.4.1. Pour les utilisateurs

Le service permet une simplification de l'accès aux applications raccordées : limitation du nombre d'authentifications et fourniture d'une interface commune d'authentification pour l'ensemble des applications rattachées sur les solutions proposées.

3.4.2. Pour les gestionnaires d'application

1) Apports du type SSO basique

- Délégation de la phase d'authentification auprès du service pour les applications. Les gestionnaires n'ont pas besoin de gérer cette phase au sein de leurs applications ;
- Augmentation du niveau de sécurité de la phase d'authentification en limitant la diffusion du login/mot de passe ;
- Intégration des applications au SI : partage de la même interface d'authentification.

2) Apports du type SSO avancé

- Apports du type SSO Basique.
- Simplification de raccordement par délégation du client SSO à un composant intermédiaire (reverse proxy : voir annexe §8.2).

3) Apports du type SSO étendu

- Apports du type SSO Basique ;
- Évite l'enregistrement des utilisateurs des partenaires INRAE dans les référentiels INRAE et la multiplication des comptes grâce à l'utilisation des référentiels partenaires ;
- Fourniture d'attributs aux applications par les référentiels utilisateurs INRAE et partenaires.

3.5. Périodes de service et qualité de service

Ce paragraphe présente la période d'ouverture et les indicateurs de qualité du service « authentification unique pour les applications web » sur lesquels le responsable du service s'engage.

Le périmètre des engagements est uniquement applicable aux solutions techniques sous la responsabilité du fournisseur de services ; les indicateurs ne prennent pas en compte les perturbations constatées sur les services utilisés par l'authentification unique (réseau, référentiels agents INRAE et partenaires, etc.)

3.5.1. Pour les incidents

Indicateur	Définition	Valeur	Commentaire
Période d'accès au service	Plages horaires pendant lesquels le service est ouvert aux applications	24h/24	Sans garantie de traitement des incidents hors heures ouvrées
Temps de prise en compte d'incidents	Délai de pris en compte d'un incident par le fournisseur du service à partir de la détection ou de la soumission de l'incident	4 heures ouvrées ¹	Taux de respect à 80%
Délai de communication en cas de perturbation	Délai que se donne le fournisseur du service pour communiquer sur la perturbation auprès de ses clients à partir du constat de cette dernière	Immédiat à partir du constat de la perturbation pendant les heures ouvrées ¹	
Taux de disponibilité de service	Taux de disponibilité du service sur les plages d'accès de ce dernier	Donnée calculée a posteriori sur une période définie	Pas d'engagement sur la disponibilité de service

3.5.2. Pour les changements

Indicateur	Définition	Valeur	Commentaire
Gestion des changements mineurs (sans coupure de service)	Plages horaires d'intervention pour un changement mineur (sans coupure de service)	6h-22h jours ouvrés ¹	

¹ Jours ouvrés, heures ouvrées : du lundi au vendredi, de 9h à 17h

Gestion des changements majeurs planifiés	Plages horaires d'intervention pour les changements majeurs planifiés	6h-9h jours ouvrés ¹ ou week-end	
Délai de communication d'un changement mineur	Délai entre la communication d'un changement mineur auprès des clients et l'intervention du changement	2 jours ouvrés ¹	Taux de respect à 80%
Délai de communication d'un changement majeur	Délai entre la communication d'un changement majeur auprès des clients et l'intervention du changement	2 mois	Taux de respect à 80%

3.5.3. Pour les demandes initiales de raccordement ou de modification

Indicateur	Définition	Valeur	Commentaire
Délai d'accusé réception d'une demande de raccordement	Délai maximum que se donne le fournisseur pour accuser réception d'une demande de raccordement	2 jours ouvrés ¹	Taux de respect à 80%
Délai d'analyse de la demande de raccordement	Délai maximum que se donne le fournisseur pour analyser le dossier de demande de raccordement	4 semaines	Taux de respect à 80%
Délais de support pour l'intégration	Délais de prise en compte et de traitement lors d'une demande de support pour l'intégration d'une application au service	Prise en compte des demandes : 2 jours ouvrés ¹ . Traitement de la demande : 2 jours ouvrés ¹ après délai de prise en compte.	Le délai total pour une intégration dépend de l'application et le type de service choisi. Les délais de raccordement SSO basique et SSO avancé sont en général plus courts que le raccordement pour le SSO étendu

4. Solutions disponibles et critères d'éligibilité au raccordement

4.1. Aperçu des solutions disponibles

Le service proposé est décliné en trois solutions techniques, qui correspondent aux trois types de service présentés plus haut.

Définition des niveaux de complexité :

- + = faible : pas besoin de compétences particulières
- ++ = moyen : connaissances dans le domaine SSO
- +++ = fort : maîtrise dans le domaine SSO

Type de service	Solutions Techniques	Le(s) référentiel(s) utilisateurs	Niveau de complexité	Principales activités du raccordement pour le client
SSO basique	WebSSO CAS	Référentiel Inra (LDAP)	client : ++ service : +	Implémenter un client WEBSSo (il existe des clients multiples pour se raccorder sur la solution retenue)
SSO avancé	WebSSO Reverse Proxy CAS	Référentiel Inra (LDAP)	client : + service : ++	Configurer la délégation de l'authentification.
SSO étendu	Fournisseur de ressources Inra au sein de la fédération Education-Recherche	Référentiel Inra (LDAP) et les référentiels des partenaires	client : +++ service : ++	Implémenter un client de la solution. Expliquer le chiffrement du niveau de complexité

4.2. Critères d'éligibilité au raccordement pour les applications

Une application sera éligible une fois vérifiés les pré-requis généraux et les critères spécifiques.

4.2.1. Prérequis généraux au raccordement pour les applications

Les prérequis pour le raccordement des applications souhaitant déléguer leur authentification des utilisateurs sur le service sont :

- INRAE doit être propriétaire ou avoir un droit d'accès contractualisé à l'application.
- Au moins un gestionnaire pour l'application concernée et un référent technique (INRAE ou non INRAE) doivent être identifiés pour l'application concernée par la demande de raccordement au service d'authentification unique (cela peut être la même personne).

Les solutions proposées pour faciliter l'authentification unique ne nécessitent pas d'environnement spécifique pour se raccorder au service.

4.2.2. Critères spécifiques au type de service « SSO avancé »

Ce type de service est disponible uniquement pour les applications hébergées sur le centre sur lequel est installé le service d'authentification, c'est à dire Jouy-en-Josas, pour des raisons techniques.

4.2.3. Critères spécifiques au type de service « SSO étendu »

Les partenaires Éducation-Recherche doivent être inscrits auprès de la fédération d'identité Éducation-Recherche.

4.3. Principes de délégation de l'authentification

4.3.1. Principes communs aux solutions techniques

Les principes communs sont les suivants :

- Le référentiel d'authentification des utilisateurs INRAE s'appuie sur le service d'annuaire LDAP de l'institut. La gestion des login et des mots de passe est à la charge de ce service.
- Les applications raccordées à ce service délèguent intégralement la gestion de l'authentification (login, mot de passe) des utilisateurs. L'application n'a pas connaissance du mot de passe de l'utilisateur qui souhaite accéder à l'application.
- La relation entre la gestion interne des utilisateurs (profil applicatif) au sein de l'application et l'authentification est facilitée par la transmission de l'identifiant de l'utilisateur à l'application.
- Le raccordement au service est compatible avec l'interrogation d'autres référentiels (référentiel Agent, référentiel Structure, référentiel Activités, ...), permettant de récupérer des attributs complémentaires. L'implémentation de cette fonctionnalité au sein de l'application cliente est soumise à validation auprès des administrateurs de ces référentiels, puis à la charge du gestionnaire d'application.

4.3.2. Principes SSO Basique

La délégation peut être réalisée directement par l'application (client embarqué dans l'application ou développement spécifique), ou par l'intermédiaire d'un proxy web qui joue le rôle du client WEBSSO.

4.3.3. Principes SSO Avancé

Cette solution permet un déport de la partie cliente du service SSO sur un dispositif mutualisé pour les applications raccordées (reverse proxy CAS).

Elle permet également de bénéficier d'un contrôle d'accès (habilitation) à partir d'attributs décrits dans le paragraphe 3.2.2

4.3.4. Principes SSO Étendu

Ce type de service permet l'utilisation des référentiels d'utilisateurs des partenaires inscrits auprès de la fédération Éducation-Recherche pour accéder aux applications INRAE.

Dans ce cadre, les applications qui le souhaitent peuvent utiliser des attributs listés dans le paragraphe §3.2.3.

La délégation peut être réalisée directement par l'application (client embarqué dans l'application). Si l'application n'embarque pas de client, la bonne pratique consiste à utiliser un proxy web qui joue le rôle de client.

5. Contacts et rôles

5.1. Contacts clients

Dans le cadre de la fourniture du service, le Client s'engage à mettre en place les contacts suivants :

- **Le gestionnaire d'application**, qui assure :
 - La contractualisation du service ;
 - Le respect des engagements relatifs au contrat ;
 - La communication auprès des utilisateurs de l'application sur les moyens déployés sur l'authentification ;
 - Le rôle de point de contact pour le responsable du service d'authentification.
- **Le référent technique**, qui assure :
 - Le raccordement de l'application au service ;
 - Le maintien en condition opérationnelle du composant de l'application qui gère l'authentification ;
 - L'expertise technique sur le raccordement.

5.2. Contacts fournisseur

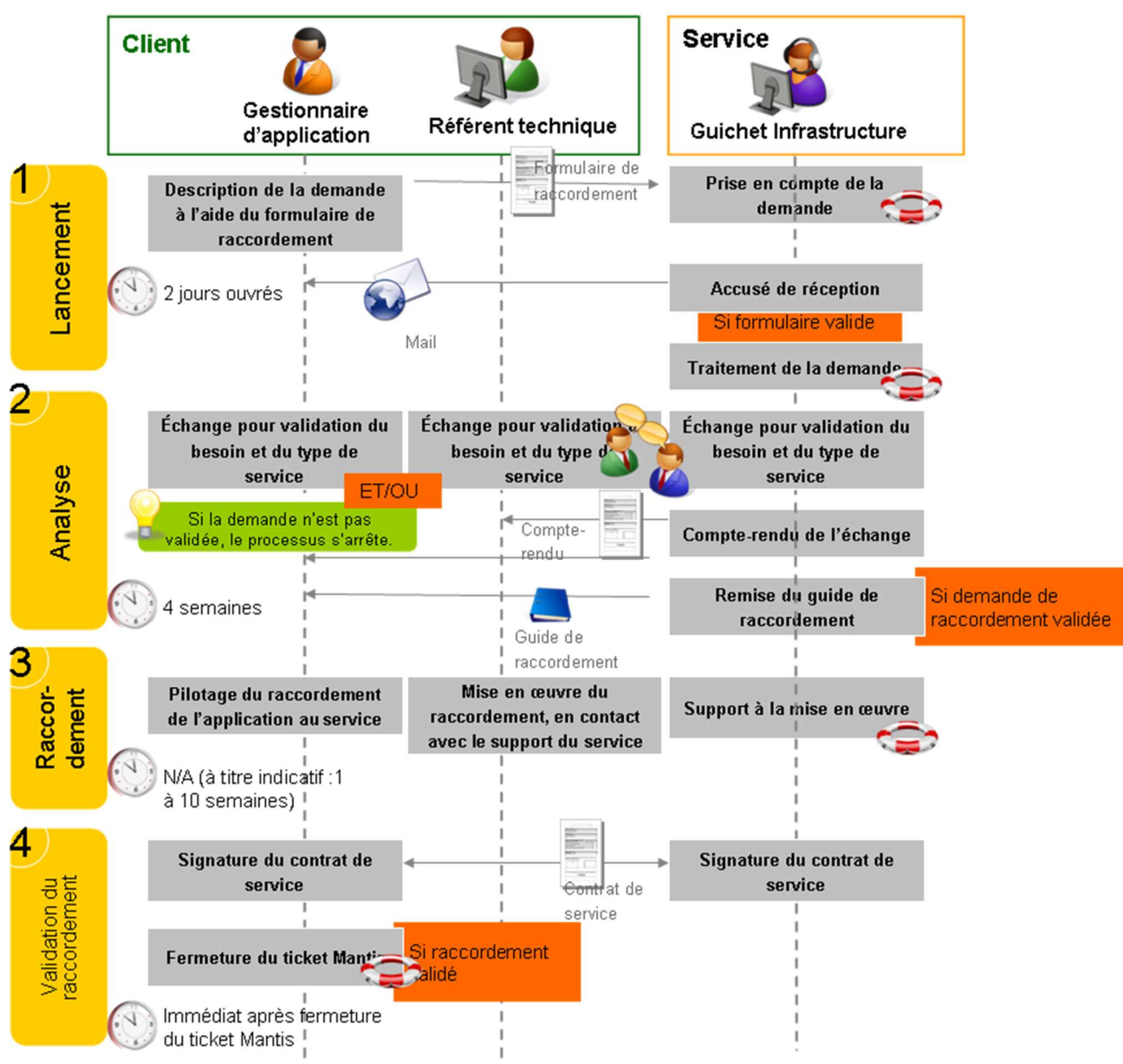
Par ailleurs le fournisseur met à disposition du client les deux contacts suivants :

- **Le guichet infrastructure** : point de contact opérationnel unique, il est chargé des différentes interactions avec le client dans le cadre des processus décrits ci-dessous.
- **Le responsable de service** : il porte la responsabilité du service et est garant de son bon fonctionnement. Il est le contact pour toute question contractuelle.

6. Processus de livraison et de gestion du service

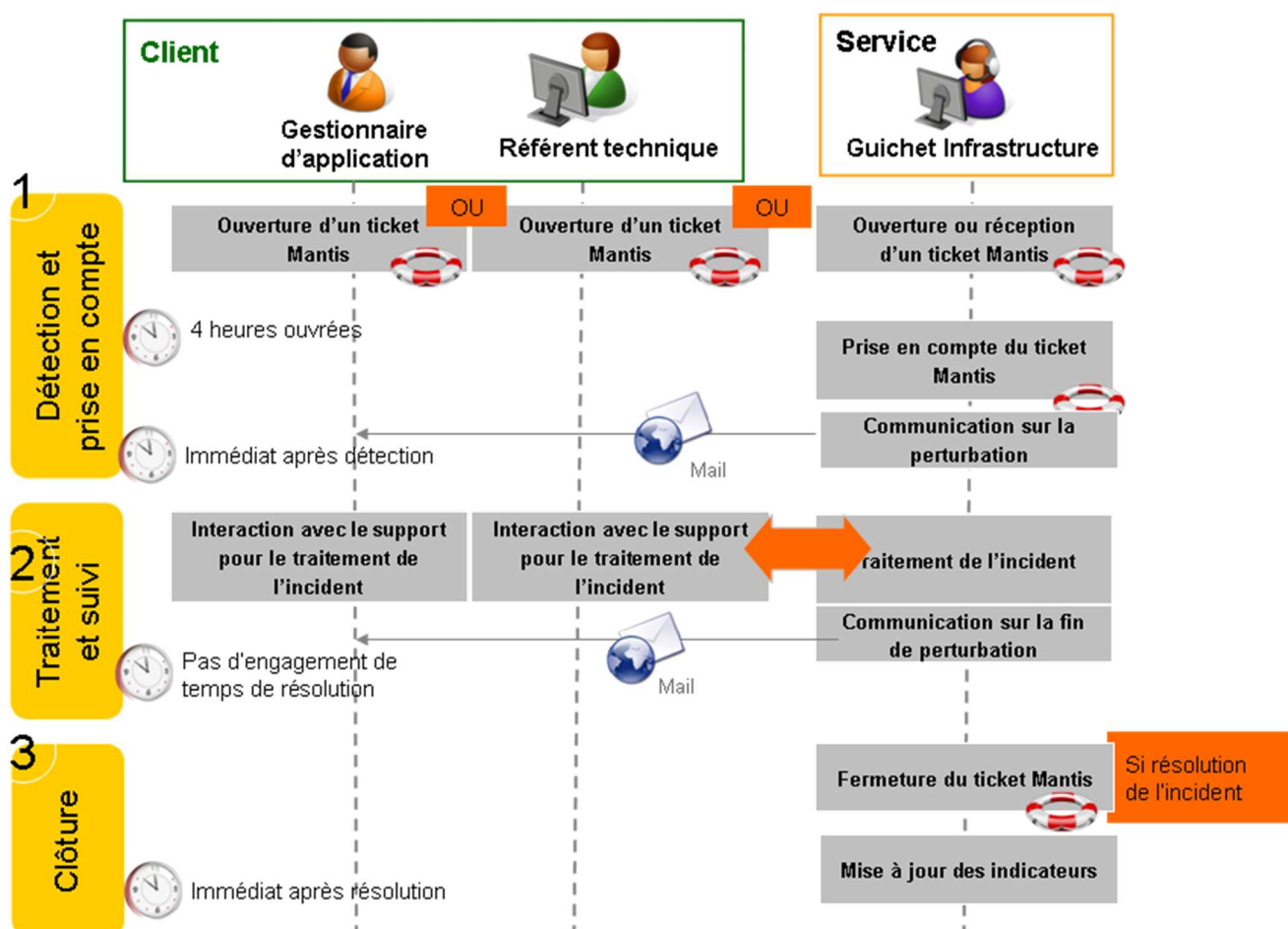
Ce chapitre décrit les processus de mise en place et de gestion du service. Les processus décrits ici traitent principalement des interactions entre le Client et le Fournisseur : certaines actions ne sont pas détaillées ici, car étant purement de la responsabilité de l'une ou l'autre des parties.

6.1. Processus de traitement d'une demande initiale ou de modification



Étapes	Acteurs	Activités/Livrables	Planning
1 Lancement	<ul style="list-style-type: none"> Gestionnaire d'application Guichet Infrastructure 	<ul style="list-style-type: none"> Le gestionnaire de l'application remplit le formulaire de raccordement Le Guichet Infrastructure reçoit la demande et ouvre un ticket Mantis. Le Guichet Infrastructure envoie un mail d'accusé de réception au gestionnaire d'application qui a émis la demande. 	2 jours ouvrés
2 Analyse de la demande	<ul style="list-style-type: none"> Fournisseur de service Gestionnaire d'application Référent technique 	<ul style="list-style-type: none"> Le fournisseur de service vérifie la complétude de la demande et l'éligibilité du client, et organise le cas échéant un échange (réunion ou point téléphonique) entre les acteurs pour valider le besoin et le choix du type de service. Le fournisseur réalise un compte-rendu de l'échange et l'envoie au gestionnaire d'application et au référent technique. Si la demande de raccordement est validée, le fournisseur fournit le guide de raccordement de la solution retenue au gestionnaire d'application. 	4 semaines
3 Raccordement de l'application	<ul style="list-style-type: none"> Fournisseur de service Gestionnaire d'application Référent technique 	<ul style="list-style-type: none"> Le gestionnaire d'application pilote la mise en œuvre du raccordement de l'application au service. Le référent technique réalise la mise en œuvre du raccordement. Il s'appuie sur le support fourni par le service. <p><u>Remarque</u> : pour un raccordement auprès de la fédération Éducation –Recherche (type de service « SSO étendu »), le fournisseur de service réalise l'enregistrement auprès de Renater.</p>	1 à 10 semaines (dépend de la solution retenue)
4 Validation du raccordement	<ul style="list-style-type: none"> Gestionnaire d'application Fournisseur de service 	<ul style="list-style-type: none"> S'il valide le raccordement, le gestionnaire d'application ferme le ticket Mantis. Le responsable du service et le gestionnaire d'applications signent le contrat de service. 	Immédiat après l'étape 3

6.2. Processus de gestion des incidents



Étapes	Acteurs	Activités/Livrables	Planning
1 Détection et prise en compte de l'incident	<ul style="list-style-type: none"> Gestionnaire d'application Référent technique Guichet Infrastructure 	<ul style="list-style-type: none"> Un ticket Mantis est ouvert par l'un des acteurs (client ou fournisseur) Le guichet Infrastructure prend en compte le ticket Mantis. Si une perturbation est d'ores et déjà constatée, le guichet Infrastructure envoie un mail de communication à tous les gestionnaires d'application clients du service. 	<p>Temps de prise en compte du ticket Mantis : 4 heures ouvrées</p> <p>Délai de communication en cas de perturbation : immédiat après la détection</p>
2 Traitement et suivi	<ul style="list-style-type: none"> Fournisseur du service Gestionnaire d'application Référent technique 	<ul style="list-style-type: none"> Le fournisseur qualifie et traite l'incident, en collaboration avec le gestionnaire d'application et le référent technique. Le Fournisseur de service interagit avec le gestionnaire d'application et le référent technique pour traiter l'incident. Si les actions correctives doivent créer une perturbation (arrêt momentané du service...), le guichet Infrastructure envoie un mail de communication à tous les gestionnaires d'application clients du service. 	<p>Délai de communication en cas de perturbation : immédiat après la détection</p>
3 Clôture	<ul style="list-style-type: none"> Guichet Infrastructure Pôle Exploitation Gestionnaires du service 	<ul style="list-style-type: none"> Si l'incident est résolu, le fournisseur de service ferme le ticket Mantis, en accord avec le client. Le guichet Infrastructure met à jour les indicateurs. 	<p>Immédiat après résolution de l'incident</p>

6.3. Processus de gestion des évolutions et des changements

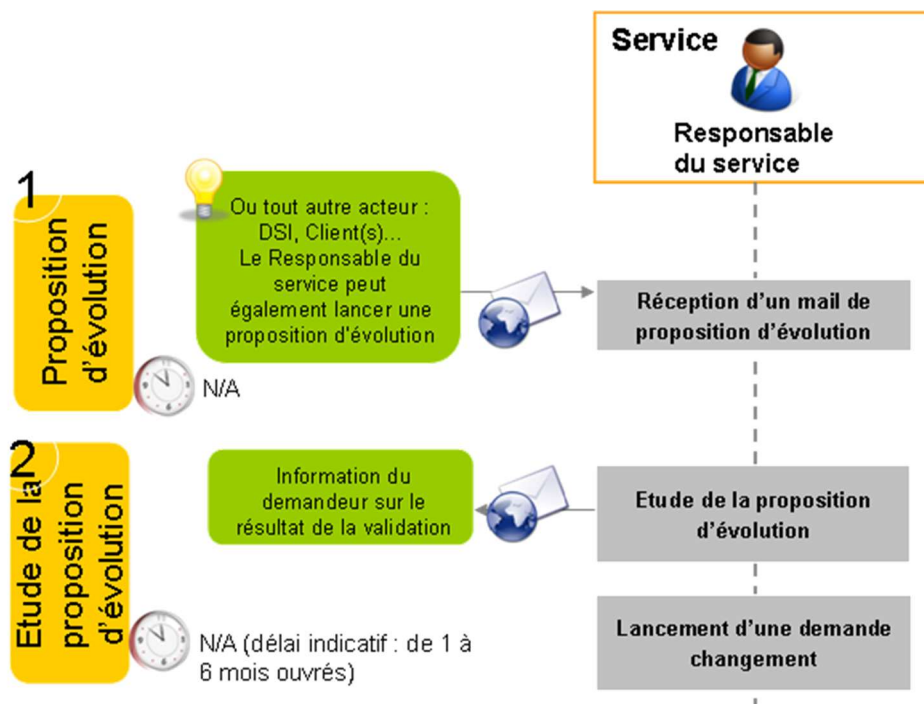
En cas de nouveau besoin (nouvelle fonctionnalité, changement technique ou fonctionnel), le Client peut faire une demande d'évolution auprès du fournisseur de service, suivant le processus décrit plus bas.

Par ailleurs, tout changement effectif sur l'infrastructure du service est traité dans le cadre de processus spécifiques. Ces changements sont de différentes natures :

- Mise en place d'une évolution (ajout, modification, retrait de fonctionnalité) ;
- Montée de version logicielle, patch de sécurité pour une solution retenue ;
- Correction d'anomalies sur les solutions déployées ;
- Changements imposés par la fédération Éducation-Recherche :
 - Montée de version de notre infrastructure pour rester compatible avec la fédération Éducation-Recherche et nos partenaires ;
 - Diffusion d'attributs complémentaires pour l'accès à des ressources hors INRAE.

Les changements sur les solutions proposées au sein du service devront être validés par le responsable du service.

6.3.1. Évolutions



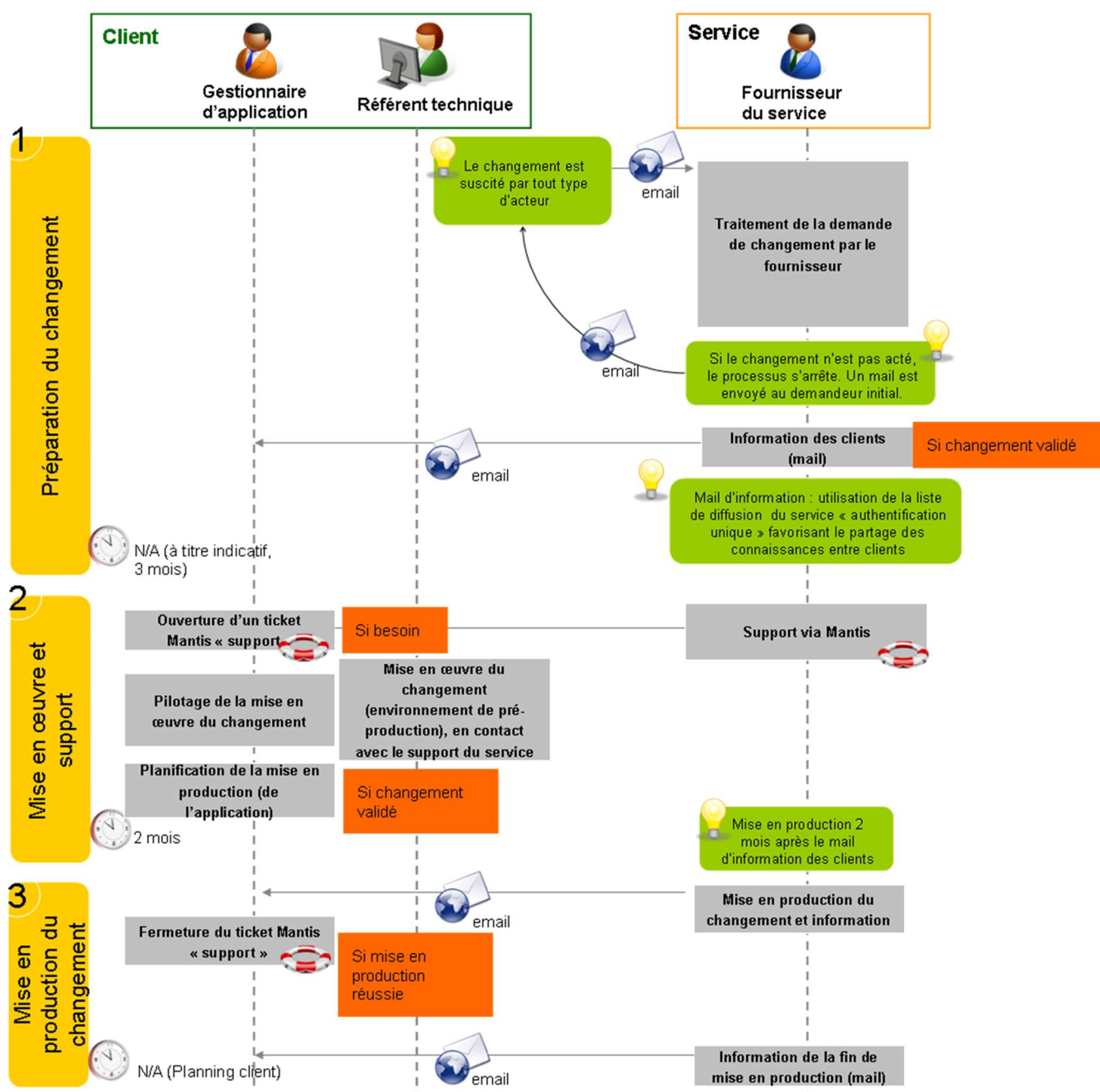
Étapes	Acteurs	Activités/Livrables	Planning
1 Proposition d'évolution	<ul style="list-style-type: none"> Tout acteur (Client ou Fournisseur) 	<ul style="list-style-type: none"> Un mail détaillé contenant la proposition d'évolution est envoyé par le demandeur au responsable du service. Ce mail doit préciser la nature de l'évolution et le besoin sous-jacent. 	N/A
2 Traitement et suivi	<ul style="list-style-type: none"> Fournisseur du service 	<ul style="list-style-type: none"> Le fournisseur étudie la proposition d'évolution : intérêt, faisabilité, risque, etc. Le fournisseur valide ou rejette la proposition. Si celle-ci est acceptée, elle fera l'objet d'une demande de changement. Le fournisseur informe le demandeur du service du résultat de la validation, quel que soit celui-ci. 	Pas de garantie de temps de traitement

6.3.2. Changements majeurs

La classification d'un changement en changement majeur est caractérisé par :

- Impact potentiel pour les applications raccordées sur le service
- Risque élevé de coupure du service lors de la mise en production

Cette classification est réalisée lors de la phase « planification et lancement » du processus.



Étapes	Acteurs	Activités/Livrables	Planning
1 Préparation du changement	<ul style="list-style-type: none"> Fournisseur de service 	<ul style="list-style-type: none"> Le changement est suscité par tout type d'acteur, ou par le responsable du service ou les gestionnaires du service. Le fournisseur du service traite la demande de changement, et prépare la mise en œuvre (impacts, documentation, test, etc.) Le Guichet Infrastructure envoie un mail d'information aux gestionnaires d'application clients du service. <p>Remarque : le mail est envoyé à la liste de diffusion du service « authentification unique » (destinée à favoriser le partage des connaissances entre clients).</p>	N/A (à titre indicatif : 3 mois)
2 Mise en œuvre et support	<ul style="list-style-type: none"> Gestionnaire d'application Référent technique Fournisseur de service 	<ul style="list-style-type: none"> Le gestionnaire d'application ouvre un ticket Mantis pour suivre la réalisation du changement dans son application. Le gestionnaire d'application pilote la mise en œuvre du changement Le référent technique réalise la mise en œuvre du changement en environnement de pré-production, à l'aide du support fourni par le service. Le Fournisseur de service suit et traite le ticket Mantis. Si le changement est validé en environnement client de pré-production, le gestionnaire d'application planifie la mise en production du changement dans son application. 	<p>Après réception du mail d'information</p> <p>Délai laissé aux applications raccordées pour mettre en œuvre les changements : 2 mois</p>

3 Mise en production du changement	<ul style="list-style-type: none"> • Référents techniques • Fournisseur du service 	<ul style="list-style-type: none"> • Deux mois après le premier mail d'information aux clients, le guichet Infrastructure renvoie un nouveau mail aux clients les informant de la mise en production du changement. • Le fournisseur réalise mise en production du changement. Les gestionnaires du service supervisent la mise en production du changement. • Le fournisseur envoie un mail aux 	N/A (selon le planning client)
------------------------------------	--	---	--------------------------------

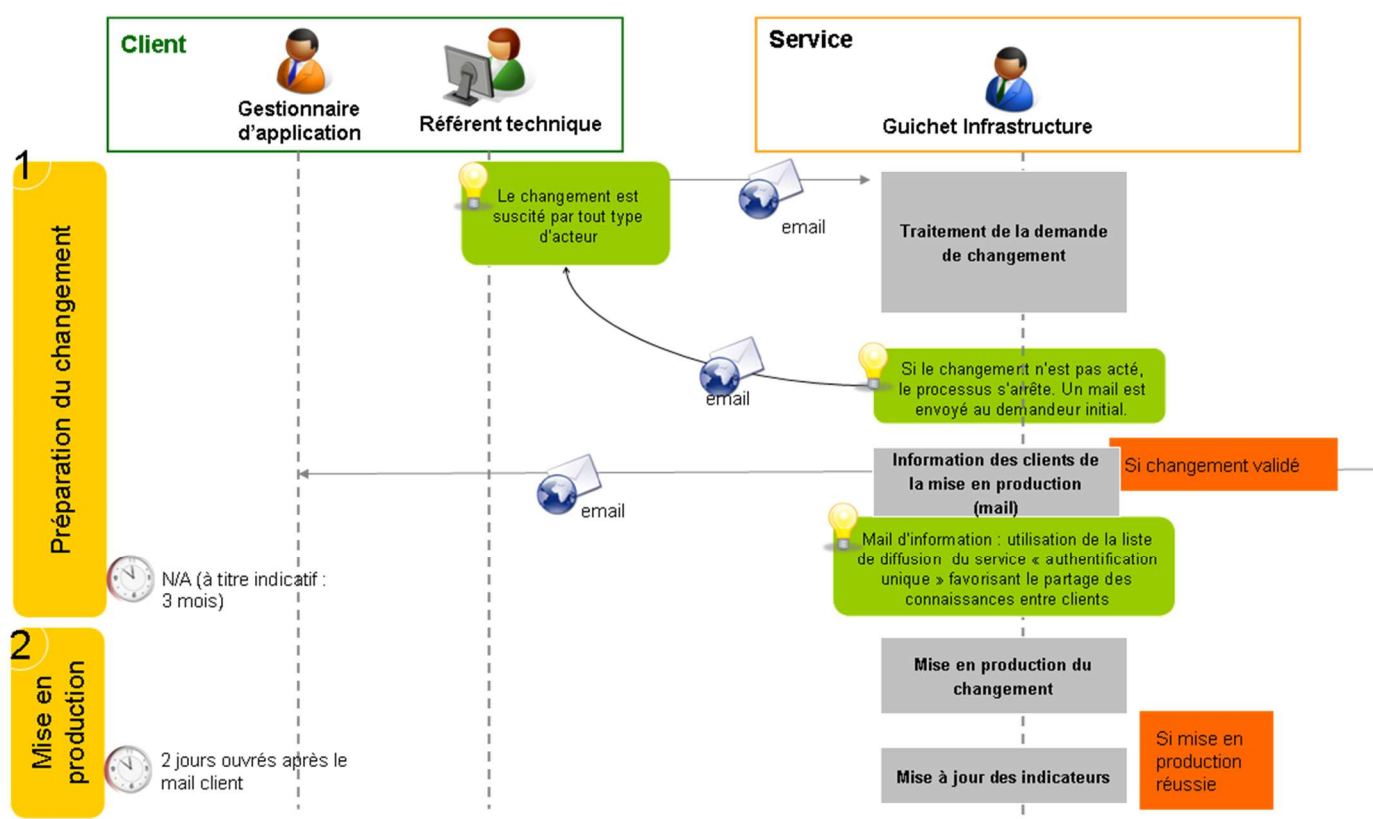
		<p>gestionnaires d'application pour indiquer la fin de la mise en production du changement.</p> <ul style="list-style-type: none"> • Une fois que la mise en production du changement dans l'application est réussie, le gestionnaire d'application ferme le ticket Mantis permettant de suivre le changement dans son application. 	
--	--	--	--

6.3.3. Changements mineurs

La classification d'un changement en changement mineur est caractérisée par les éléments suivants :

- Pas d'impact sur les applications raccordées sur le service.
- Sans interruption du service lors de la mise en production

Cette classification est réalisée lors de la phase « planification et lancement » du processus.



Étapes	Acteurs	Activités/Livrables	Planning
1 Préparation du changement	<ul style="list-style-type: none"> Fournisseur du service 	<ul style="list-style-type: none"> Le fournisseur du service traite la demande de changement, et prépare la mise en œuvre (impacts, documentation, test, etc.) Le Guichet Infrastructure envoie un mail d'information aux gestionnaires d'application clients du service. Ce mail les avertit qu'un changement au niveau du service va être mis en production deux jours ouvrés à partir de la date d'envoi du mail. <p>Remarque : le mail est envoyé à la liste de diffusion du service « authentification unique » (destinée à favoriser le partage des connaissances entre clients)..</p>	N/A (à titre indicatif : 3 mois)
2 Mise en production du changement	<ul style="list-style-type: none"> Fournisseur du service 	<ul style="list-style-type: none"> Le fournisseur de service réalise la mise en production du changement. 	2 jours ouvrés après l'envoi du mail d'information aux clients.

7. Indicateurs

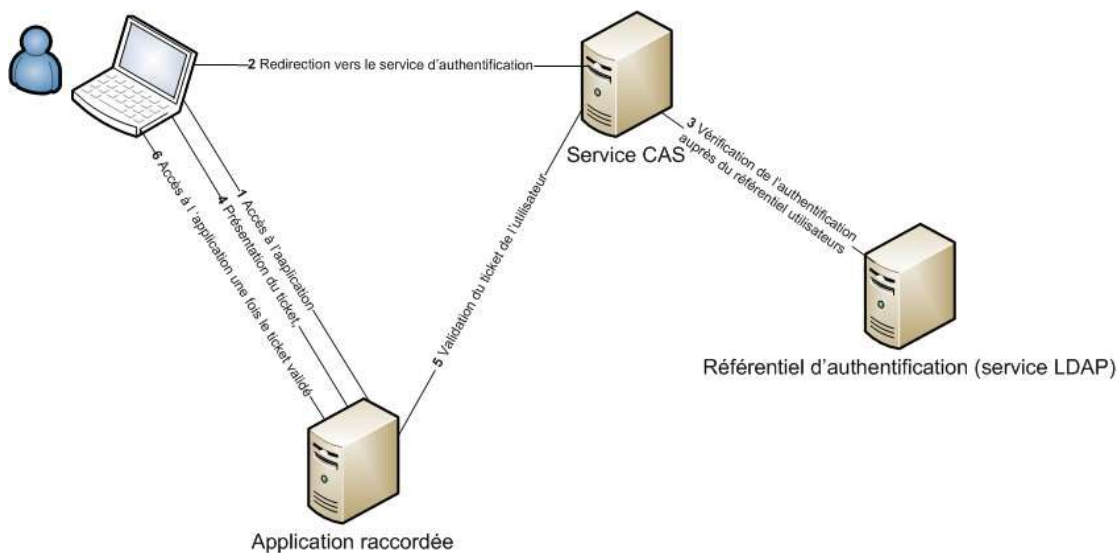
Afin de mesurer le niveau du service, le fournisseur du service s'engage à produire auprès des gestionnaires d'applications un reporting trimestriel.

Ce reporting comprend les éléments suivants :

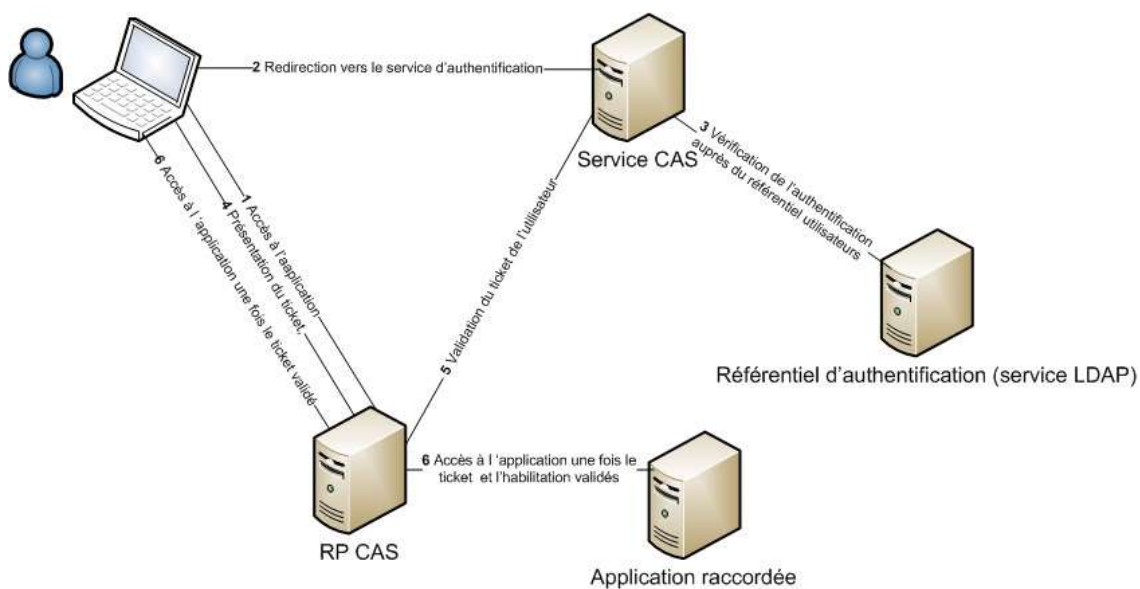
Indicateurs de niveau de service	
	Qualité de service : <ul style="list-style-type: none"> • Taux de disponibilité sur la période • Temps de prise en compte des incidents et taux de respect • Temps de résolution des incidents
	Temps de réponse moyen
	Nombre d'accès au service sur la période
	Nombre d'incidents sur la période
Indicateurs de suivi des clients	
	Nombre de demandes client en attente
	Nombre de demandes prises en compte
	Nombre de demandes en cours d'analyse
	Nombre de demandes en cours d'intégration
	Nombre de demande raccordée au service/ solutions techniques
	Nombre de demandes par mois
	Nombre d'applications raccordées par mois

8. Annexes

8.1. Schéma des composants techniques pour le type de service « SSO basique »



8.2. Schéma des composants techniques pour le type de service « SSO avancé »



8.3. Schéma des composants techniques pour le type de service « SSO étendu »

