MINISTÈRES
TERRITOIRES
ÉCOLOGIE
LOGEMENT

Liberté
Égalité
Fraternité

SERVICE CERBERE

Présentation générale

Version 4 mise à jour du
Mercredi 22 octobre 2024

Secrétariat général
Direction du numérique
Département Sécurité et gestion de crise

SOMMAIRE

1 Objet du document

Ce document présente le service CERBERE mis à disposition au sein du MTEL.

Sont détaillés ci-dessous :

- Les objectifs du service,
- L'architecture mise en place,
- Les fonctionnalités mises à disposition,
- Les différentes typologies d'utilisateurs du service,
- L'état des lieux des raccordements applicatifs réalisés,
- Les points de contact en cas de besoin.

Ce document est ensuite décliné en un ensemble de documentations techniques et fonctionnelles de la solution, ainsi qu'une aide en ligne, que ce soit pour les utilisateurs finaux ou bien les administrateurs du système.

Rédacteur : Secrétariat Général / Direction du Numérique / Département sécurité et gestion de crise / Groupe Expertise technique (DSGC/GET)

2 Objectifs du Service CERBERE

La maîtrise du cycle de vie des identités et des accès aux SI du Ministère est un élément clé pour la maitrise des risques et du niveau de sécurité.

Cette maîtrise se heurte souvent à plusieurs écueils :

- La multiplicité des sources de données d'identité numérique, pouvant être propre à chaque application accédée,
- Une non répercussion du cycle de vie des utilisateurs dans l'ensemble des systèmes (arrivée – mutation – départ)
- Une gestion des habilitations propre à chaque application, rendant compliquée la gestion globale de ces mêmes habilitations,
- Une expérience utilisateur pouvant être complexe, avec des authentifications multiples pour accéder à différentes applications chacune ayant son propre référentiel d'identification et d'habilitation.

Ainsi, le Ministère a décidé très tôt la mise en place d'un service permettant de :

- Centraliser un référentiel d'identités qui deviennent source primaire pour l'ensemble des infrastructures,
- Centraliser l'authentification des utilisateurs pour le compte d'applications raccordées au service,
- Centraliser la gestion des habilitations dans ce même service,
- Faciliter la vie des responsables applicatifs en fournissant un service d'identification, d'authentification et d'habilitation normalisé auquel raccorder les applications,
- Faciliter la vie des utilisateurs en fournissant un système de SSO (Single Sign On) évitant ainsi les réauthentifications multiples.

Ce service a été baptisé **CERBERE** et a ainsi pour objectif de :

- Fournir un service d'identification centralisé des accédants au SI,
- Fournir des interfaces permettant l'utilisation de différents protocoles d'authentification utilisés au sein du Ministère,
- Fournir un système centralisé de configuration des habilitations d'accès au parc applicatif,
- Permettre la mise en place d'une fonction de SSO pour les utilisateurs finaux,
- Permettre un raccordement facilité des applications à ce système centralisé.

L'objectif de ce produit est de raccorder l'ensemble des applications utilisées au sein du Ministère au service CERBERE.

3 Architecture fonctionnelle générale mise en place

3.1 Schéma général

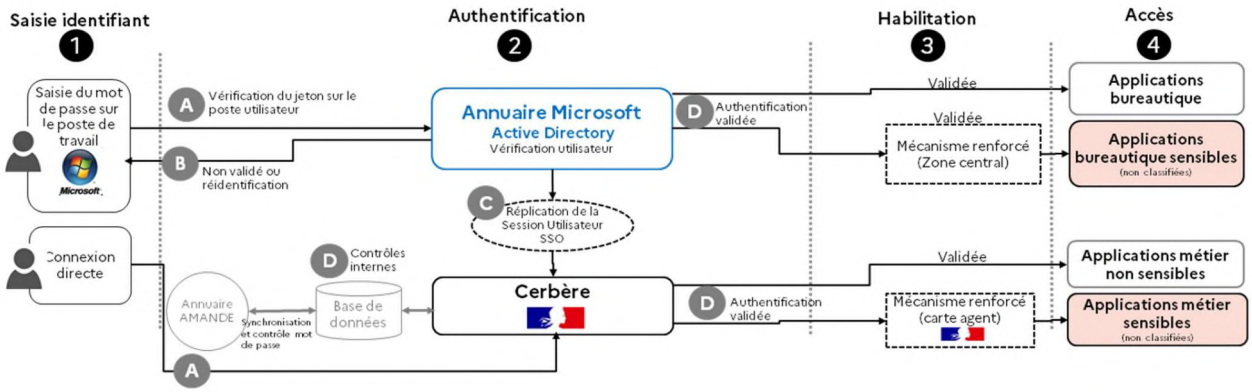
Les schémas ci-dessous présentent l'architecture générale mise en place pour rendre l'ensemble des objectifs listés précédemment.

2 briques constituent le service CERBERE :

- **1 L'accès utilisateurs** : 3 typologies d'accès permettent aux utilisateurs de s'authentifier ainsi d'accéder aux applicatifs MTEL,
  - 1/1 L'accès aux utilisateurs internes
  - 1/2 L'accès aux utilisateurs d'autres ministères
  - 1/3 L'accès aux utilisateurs externes

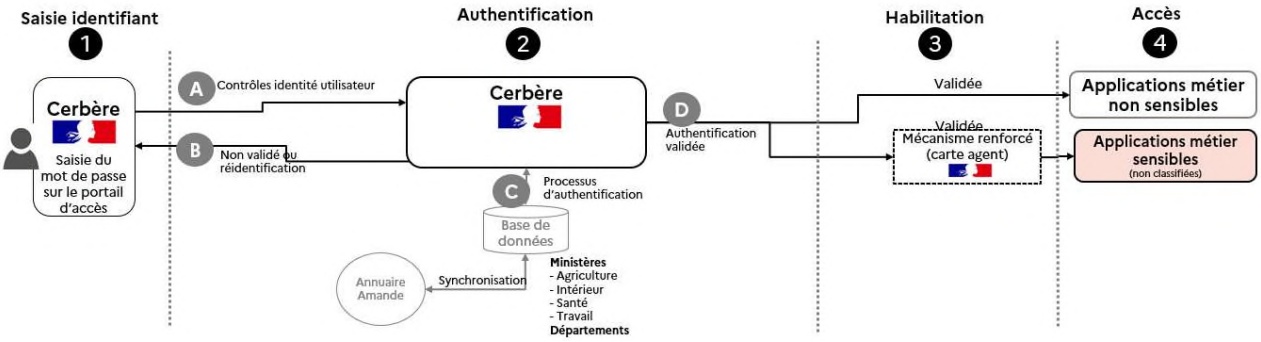
- **2 L'accès administrateurs** permettant la gestion des habilitations pour une partie du parc applicatif ainsi que la gestion des droits d'accès.
  - 2/1 Accès administrateurs
  - 2/2 API de recherches

1/1 Brique accès utilisateurs internes MTEL



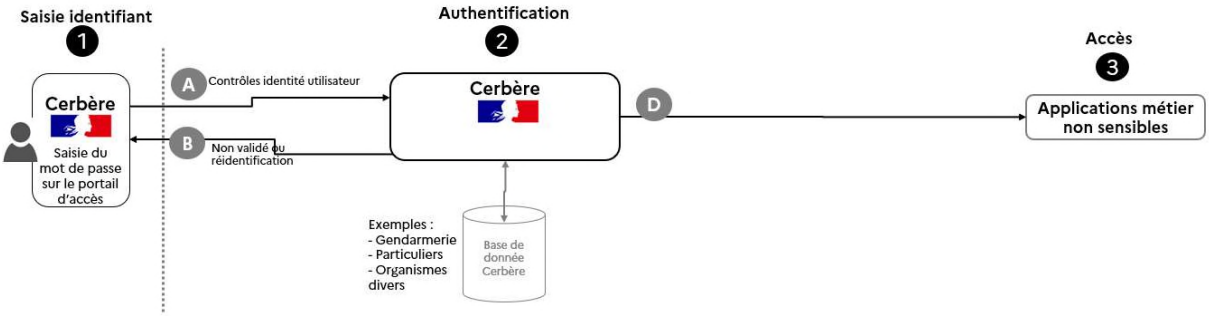
Lorsqu'un utilisateur interne MTEL se connecte à son poste de travail, son identité est d'abord vérifiée par Microsoft Active Directory puis sa session est répliquée sur Cerbère qui donne alors accès aux applications.
Dans certains cas, VPN non connecté, carte agent engagée, … l'authentification est faite directement par Cerbère.

1/2 Brique accès utilisateurs autres ministères



Lorsqu'un utilisateur d'un autre Ministère se connecte sur Cerbère son identité est alors validée via l'annuaire Amande dans laquelle l'identité a été importée par synchronisation entre annuaires.

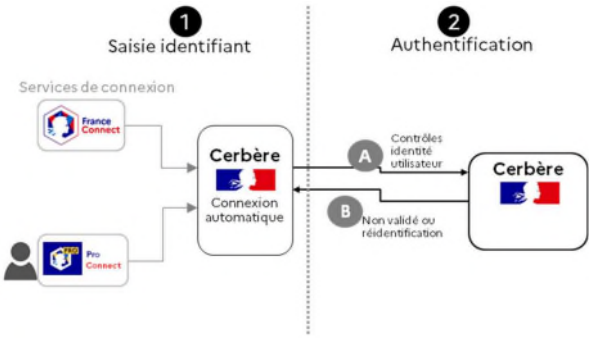
1/3 Brique d'accès utilisateurs externes



Lorsqu'un utilisateur externe se connecte sur Cerbère, son identité est validée par les éléments enregistrés par lui ou un administrateur dans la base de données Cerbère.

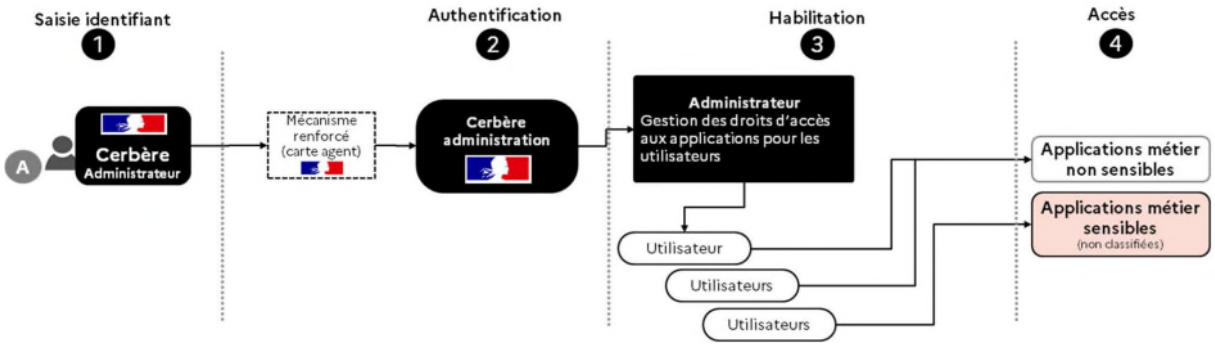
Remarques complémentaires :

1) Il est possible pour les utilisateurs de s'authentifier à Cerbère via les outils interministériel tel que **Pro Connect ou France Connect.**



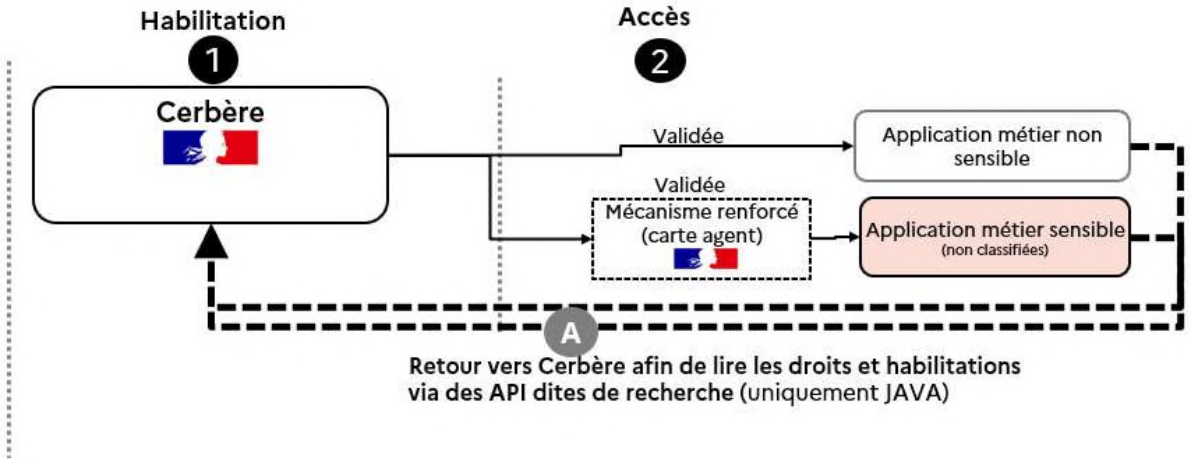
2) **Cerbère permet aussi l'usage d'autres outils d'authentification** courants tels que :
   - Yubikey
   - Fido
   - U2F
   - …

2/1 Accès administrateurs



Les administrateurs Cerbère se connectent via un portail doté d'un mécanisme d'authentification renforcé, ils peuvent alors, dans leur périmètre de compétence, définir les droits d'accès des utilisateurs aux différentes applications.

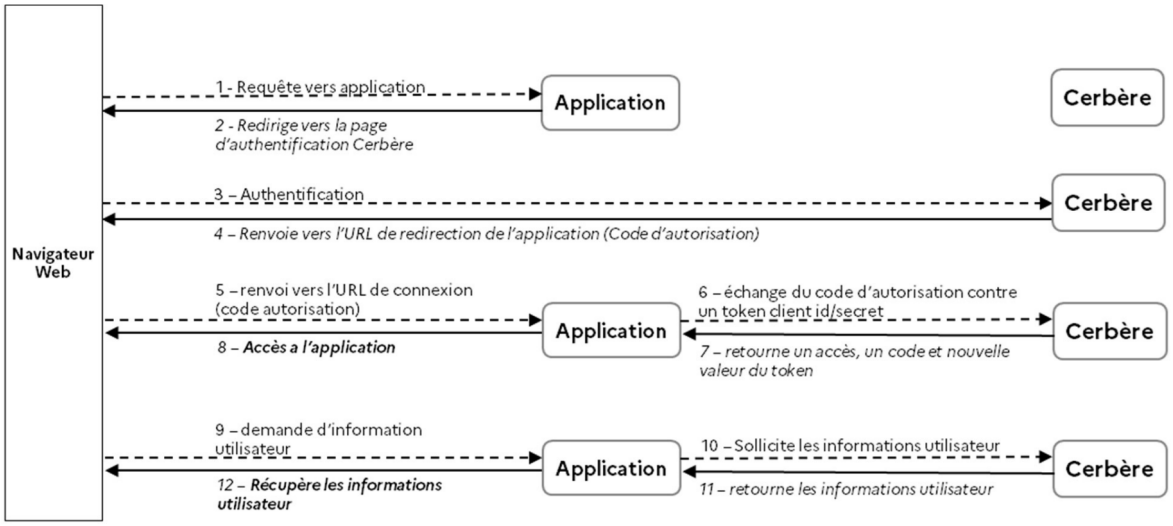
2/2 API de recherches



Les applications utilisent des API de recherches pour lire les droits paramétrés dans Cerbère.

3.2 Cinématique

La cinématique générale du service de gestion des accès est résumée dans le schéma ci-dessous.



Pour toute application connectée au service CERBERE, la gestion de l'accès d'un utilisateur dont le compte existe dans CERBERE est le suivant :

1. L'utilisateur se connecte sur l'application métier demandée,

2. L'utilisateur, n'ayant pas encore de jeton validé par CERBERE, voit sa connexion redirigée vers CERBERE de manière transparente,

3. L'utilisateur s'authentifie alors avec les moyens d'authentification mis à sa disposition,

4. Une fois l'authentification réalisée au niveau de CERBERE, une synchronisation est réalisée avec l'application, permettant l'approbation de l'accès à l'application, avec les droits associés,

5. L'utilisateur peut alors accéder à l'application demandée,

6. Ce même utilisateur peut par ailleurs accéder à d'autres applications connectées à CERBERE et nécessitant le même niveau d'authentification, sans avoir besoin de se réauthentifier, à condition que l'application autorise le SSO dans sa configuration Cerbère.

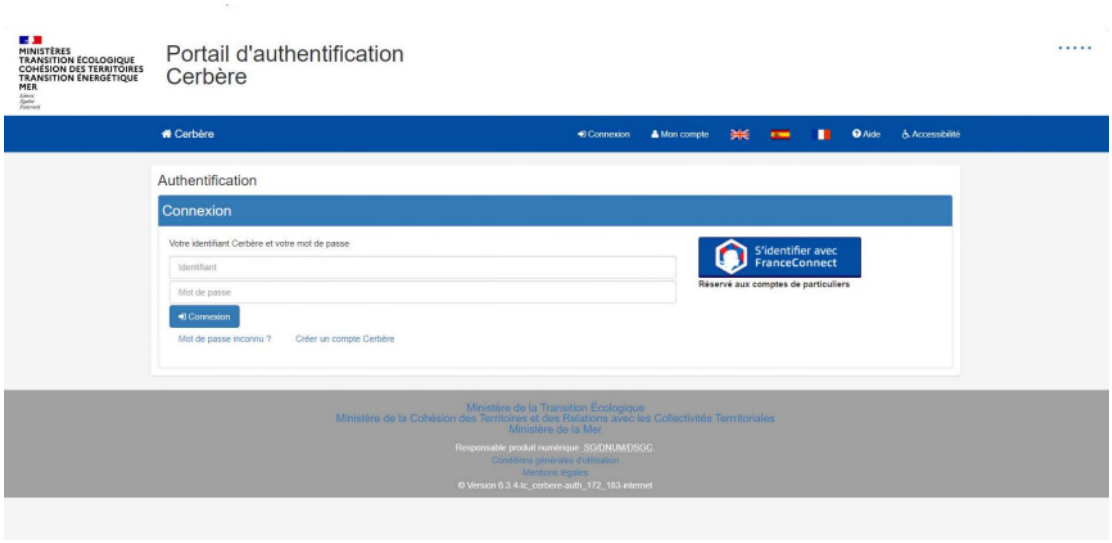
4 Services détaillés mis à disposition par CERBERE

4.1 Portail utilisateur

Le portail utilisateur permet à l'utilisateur d'être complètement autonome dans la gestion de son compte CERBERE.

Ce portail inclut les fonctionnalités suivantes :

- Auto-enregistrement pour les comptes externes qui ne peuvent être créés par synchronisation depuis l'annuaire Amande,
- Activation de son compte,
- Changement de mot de passe
- Changement de mail pour les comptes externes
- Gestion des moyens d'authentification. L'utilisateur a la possibilité de configurer les différents moyens d'authentification qu'il souhaite utiliser avec CERBERE. Les principaux moyens d'authentification mis à disposition sont notamment :
    - Carte Agent,
    - Certificat numérique,
    - Identifiant / mot de passe TOTP / HOTP avec Yubikey,
      Les typologies de moyen d'authentification évoluent en permanence au sein de CERBERE, permettant d'accompagner les évolutions technologiques.
- Se déconnecter.



4.2 Portail administrateur fonctionnel

Le portail administrateur fonctionnel permet aux administrateurs fonctionnels de configurer les accès.

Ce portail inclut notamment les fonctionnalités suivantes :

- Gestion des droits d'accès aux applications par un système de profils, permettant ainsi de configurer des habilitations orientées « métier »
- Paramétrage des modes/niveaux d'authentification minimum obligatoires pour accéder à chacun des profils d'application,
- Vérification de la création de comptes auto-enregistrés dans le portail d'authentification CERBERE,
- Gestion des comptes des administrateurs fonctionnels. Il existe au sein de CERBERE des niveaux d'administration fonctionnels différents suivant les organisations.
- Attribution de droits d'accès par défaut pour des entités de l'annuaire afin de permettre à toute une population d'utiliser certaines application généralistes (ex : gestion du temps de travail).

4.3 Service de synchronisation d'annuaire

Ce service permet la synchronisation de la base CERBERE avec des annuaires externes.

L'annuaire de référence utilisé actuellement est l'annuaire **Amande**. Le service de synchronisation permet ainsi :

- L'agrégation de l'ensemble des données identités des utilisateurs à partir de l'annuaire Amande, ces données proviennent d'une part de l'alimentation par l'application Amédée qui alimente une partie de l'annuaire Amande) et d'autres éléments provenant d'autres annuaires (autres ministères, services partenaires)

- De rendre la gestion du cycle de vie de l'utilisateur homogène au sein du Ministère. En cas de départ ou à la mutation d'un utilisateur référencé dans Amande, la synchronisation automatique avec l'annuaire Amande de CERBERE permet de désactiver les droits d'accès aux différentes applications gérées par CERBERE.

Les types de comptes gérés dans CERBERE sont les suivants :

Type de compte
Comptes Amande Mélanie 2
Importé dans l'annuaire Amande (autres ministères, organismes sous tutelle)
Autre (Créé par un administrateur dans l'ancienne application de gestion)
Particulier
Professionnel étranger
Professionnel français

4.4 Service web SIRENE

Cerbère permet un auto enregistrement d'un compte lié à une entreprise.

- Cerbère vérifie auprès de l'INSEE que le numéro SIREN de l'entreprise est valable.
- Les informations d'adresse sont alors proposées lors de l'enregistrement de l'utilisateur à partir du numéro SIREN saisi.

4.5 Service de Validation des Certificats

Le Service de Validation des Certificats permet, quand la personne se connecte, de vérifier que le certificat de l'agent n'est pas révoqué et conforme à des politiques de sécurité définies selon les autorités de certification. Ce dispositif repose sur le produit VeriCert d'EVIDEN (ATOS/BULL).
Le mécanisme de contrôle s'effectue en 2 étapes :

- Contrôle automatique des CRL (listes de révocations) lors de la connexion.
- Si le certificat est révoqué, la connexion est refusée.
- Si le certificat est valide mais pas adapté au profil visé, l'accès n'est pas autorisé.

4.6 Service de raccordement des applications

Le service de raccordement offre une interface homogénéisée de raccordement des applications au service CERBERE. Le raccordement peut être réalisé suivant différents protocoles normalisés :

- SAML version 1 (Security Assertion Markup Language)
- SAML version 2
- CAS (Central Authentication Service)
- OIDC (OpenID Connect)

DSGC préconise l'utilisation du protocole OpenID Connect **pour toutes les nouvelles applications.**

5 Utilisateurs du service CERBERE

Ce chapitre décrit les différentes typologies d'utilisateurs du service CERBERE.

5.1 Utilisateur final

L'utilisateur final voit le service CERBERE comme un portail d'authentification, lui permettant de s'identifier et s'authentifier pour accéder à un ensemble d'applications. L'interaction de l'utilisateur final avec CERBERE reste limitée à :

- L'accès au portail utilisateur lui permettant de gérer son compte,
- La réalisation d'authentification sur le portail CERBERE pour accéder à des applications.

Tout utilisateur ayant un compte dans Amande a automatiquement un compte dans CERBERE.

L'utilisateur final aura son compte bloqué en cas de tentatives erronées d'accès à son compte. Il devra alors cliquer sur « Mot de passe inconnu » pour voir son compte débloqué.

Les utilisateurs finaux de CERBERE doivent :

- Veiller à la protection des éléments leur permettant de s'authentifier,
- Signaler immédiatement toute perte de moyen d'authentification qui pourrait être réutilisé par une personne tierce,
- Ne pas communiquer ces éléments secrets permettant de s'authentifier sur CERBERE,
- Signaler toute anomalie sur leur compte.

5.2 Maitrise d'ouvrage applicative.

Les maitrises d'ouvrage applicatives interagissent avec les services CERBERE :

- Lors de la définition du raccordement entre l'application visée et CERBERE,
- Lors de la gestion du cycle de vie du raccordement, dans le cas d'évolutions :
  - De l'application,
  - Des profils d'accès à l'applications,
  - D'évolutions de CERBERE.

Les rôles et responsabilités de la maitrise d'ouvrage applicative sont de :

- Définir avec les équipes CERBERE le mode de raccordement le plus approprié,
- Définir les profils d'accès à l'application à configurer dans CERBERE,
- Définir les règles d'attribution des profils en fonction des populations visées,
- Définir le processus de validation des attributions de profils (manuel, par autorisation d'entité (automatique), à plusieurs niveaux (Administrateur d'application National ou bien Administrateurs de service déconcentré…).

5.3 Administrateurs fonctionnels

Les administrateurs fonctionnels procèdent à la configuration des accès via l'utilisation de profils attribués aux utilisateurs finaux.
Il existe 2 profils d'administrateurs fonctionnels :

- Chargés d'application Nationaux : qui créent des accès spécifiques au niveau d'un seul applicatif (en général au niveau d'une MOA ou d'une équipe d'assistance)
- Administrateurs de services : qui créent des accès pour plusieurs applications au niveau d'un service (par exemple en DDT ou en DREAL)

Les rôles et responsabilités des administrateurs fonctionnels sont de :

- S'assurer de l'adéquation des profils d'accès configurés par rapport aux exigences métiers remontées par les responsables applicatifs,
- Valider la création de nouveaux comptes sur leur périmètre,
- Valider l'attribution d'habilitations,
- Gérer la sécurité des comptes par des revues de droits.

5.4 Administrateurs nationaux

Les administrateurs nationaux interviennent dans le maintien en conditions opérationnelles de la plateforme.

Les rôles et responsabilités des administrateurs techniques sont de :

- S'assurer du bon fonctionnement des différents modules,
- Gérer les montées de version,
- Qualifier, en support niveau 3, les anomalies remontées et, le cas échéant, les résoudre ou proposer un plan de marche permettant de résoudre l'anomalie remontée.

6 Etat des lieux des applications raccordées

Cerbère permet :

- L'identification / authentification pour plus de 1000 applications du Ministère.
- La gestion des droits pour 284 applications majeures.

7 Points de contact

Vous souhaitez en savoir plus sur CERBERE ? Vous souhaitez raccorder une application ?

Plusieurs points de contact et centre d'aide :

- Support utilisateurs Cerbère : Demandes - Assistance Produits de Sécurité - Portail Support Produits et Services (developpement-durable.gouv.fr)
- Lien vers la page DSGC : [Produit sécurité] CERBERE (authentification) | Métiers du numérique SG/DNUM (rie.gouv.fr)