Convention d’utilisation  
(Services web BOSA DT sur FSB ou services FSB)

Objectif du document:

Une convention d'utilisation est un contrat spécifique à un service qui stipule les conditions liées à l'utilisation d'un service spécifique de BOSA DT.

Il s’agit d’un document formel signé par les responsables des Parties qui souhaitent utiliser le service (« utilisateurs »). En signant une convention d'utilisation, l'utilisateur se déclare d'accord avec les conditions générales des services de BOSA DT.

**1/01/2019**

SPF BOSA – DG Transformation Digitale

Version : 1.3

TABLE DES MATIERES

[1. Conditions spécifiques 3](#_Toc3562485)

[1.1 Description et fonctionnement du service 3](#_Toc3562486)

[1.1.1 Fonctionnement du service 3](#_Toc3562487)

[1.2 Utilisation du service 5](#_Toc3562488)

[1.2.1 Plan pas à pas pour la connexion à un service FSB 5](#_Toc3562489)

[1.2.2 Rôles et responsabilités 6](#_Toc3562490)

[1.2.3 Coûts liés à l’utilisation du service 7](#_Toc3562491)

[1.3 Sécurité 7](#_Toc3562492)

[1.3.1 Sécurisation du FSB 7](#_Toc3562493)

[1.3.2 Sécurisation de l’utilisateur final 7](#_Toc3562494)

[1.3.3 Finalité 8](#_Toc3562495)

[1.3.4 Audittrail 8](#_Toc3562496)

[2. Niveaux de service 9](#_Toc3562497)

[2.1 Disponibilité 9](#_Toc3562499)

[2.1.1 Disponibilité du service 9](#_Toc3562500)

[2.1.2 Capacité et performance 10](#_Toc3562501)

[2.2 Niveaux de service 11](#_Toc3562502)

[2.3 Support 11](#_Toc3562503)

[2.4 Rapports et evaluation 13](#_Toc3562504)

[2.5 Modification des niveaux de service 13](#_Toc3562505)

[3. Parties et signature 14](#_Toc3562506)

# Conditions spécifiques

## Description et fonctionnement du service

### Fonctionnement du service

DESCRIPTION

Les services web présents sur le Federal Service Bus (FSB), aussi nommés « Services FSB », ont pour but d’améliorer l’accessibilité aux principales sources authentiques (SA). Concrètement, BOSA DT met à la disposition des utilisateurs une plate-forme permettant la consultation ou l’échange standardisé de données, d’une application à l’autre, par Internet. La plate-forme met à disposition de manière homogène et sécurisée des services web qui offrent un accès aux sources authentiques.

Les sources authentiques sont également appelées « service providers ».

Les utilisateurs sont parfois appelés « service consumers ».

Les services web sont développés sous la forme de composants réutilisables. Ils se révèlent particulièrement utiles en tant que composants de base simplifiant le développement de guichets virtuels.

Le catalogue des services web peut être consulté en ligne sur le « FSB Registry ». D’autres services web pourront être ajoutés à la demande des utilisateurs.

Les services web sont regroupés en familles de services web. Une famille de services web est un ensemble logique de services web. Une famille est constituée de services web liés entre eux par leur contenu fonctionnel et/ou par la source authentique.

Dans le cadre de ces services, BOSA DT se charge des aspects suivants :

* la mise à disposition du FSB ;
* la gestion opérationnelle et la gouvernance du FSB ;
* la publication d’un catalogue de services web et des informations techniques afin de permettre l’accès à ces services ;
* le support dans le cadre du calibrage et de l’utilisation des services web.

FONCTIONNEMENT

Le FSB permet de tracer des voies de communication simplifiées à valeur ajoutée non seulement entre les applications publiques, mais aussi entre ces dernières et les applications de leurs partenaires.

Les sources authentiques ou *service providers* mettent leurs applications à la disposition du FSB par le biais de services web (ou d’un autre protocole), appelés « services SA ». Selon les besoins des utilisateurs, ces services SA seront présentés de différentes manières sur le FSB, et ce, sous forme de services web : il s’agit des « services FSB ».

Un service FSB peut se composer de plusieurs services SA sous-jacents présentés comme un service web unique aux utilisateurs. L’ouverture d’accès au Registre national et au Registre Bis en est un bel exemple. Le FSB offrira un PersonService afin de permettre à l’application de l’utilisateur de rechercher des données sur une personne physique. Le service FSB peut effectuer une recherche, visible par l’application de l’utilisateur, à la fois dans le Registre national et le Registre Bis. Les résultats sont regroupés et transmis à l’application de l’utilisateur. L’application de l’utilisateur ne doit pas connaître la complexité sous-jacente. Le FSB contribue ainsi à la simplification administrative.

Ce procédé permet de réaliser des projets réunissant plusieurs administrations ou partenaires et offrant à ces derniers une grande indépendance.

**Du point de vue de la source authentique ou *service provider***

Les services publics peuvent eux-mêmes déterminer comment concevoir et gérer leurs sources (authentiques) et comment y donner accès (ils développent en effet eux-mêmes le service prévoyant les fonctionnalités de base du service FSB auquel ils participent).

Par le biais des processus de gouvernance du FSB, on détermine et vérifie quels utilisateurs utiliseront les services SA. Cette méthode offre au service public responsable de la SA (et à BOSA DT pour son FSB) la possibilité de planifier les ressources.

Le FSB se charge d’authentifier les applications des utilisateurs et de contrôler l’accès aux services FSB.

**Du point de vue de l’utilisateur ou *service consumer***

Les utilisateurs peuvent quant à eux créer leurs applications en toute indépendance. Les services FSB utilisables, accompagnés d’une explication sur leur mode d’intégration, sont consultables dans le *FSB Registry*.

Étant donné que les services du FSB sont techniquement uniformes, les utilisateurs peuvent se prévaloir de l’expérience qu’ils ont acquise dans des projets antérieurs.

CARACTERISTIQUES

* Le FSB permet une **approche de projets orientée sur les services.**

Cette approche est dite « orientée sur les services » d'une part parce que les composants de base du modèle sont appelés « services » et d'autre part parce que la forme de collaboration implique cette « orientation sur les services ».

La communauté de *service providers* donne accès à ses propres applications dès qu’elle estime qu’elle peut ainsi rendre service à la communauté des utilisateurs (réduire leur charge de développement, encourager la collaboration, etc.).

* Le FSB rend **moins dépendante de la technologie l’ouverture d’une source authentiqu**e (ou l’intégration entre services en général).

Les efforts d’intégration au FSB (l’ensemble des mesures techniques devant être prises pour se connecter) sont moins considérables que ceux fournis pour l’UME.

* Le FSB nécessite nettement **moins de dépendances mutuelles entre source authentique et utilisateur** (« loose coupling »).  
    
  Le FSB permet à l’utilisateur de se connecter au service FSB, quasi sans interaction avec la source authentique du service SA sous-jacent. D’un point de vue technique, l’utilisateur ne doit pas connaître le responsable de la source authentique : la connexion technique elle-même (au service FSB), l’authentification et l’autorisation sont réglées entre l’utilisateur et le FSB. Cette propriété permet également de dissimuler ou de limiter l’impact des adaptations aux services SA.
* Le FSB est basé sur des **standards ouverts** tels que SOAP, WSDL, UDDI, WS-Security, XSD et HTTP/S.
* Il offre un éventail de **fonctionnalités**:
  + **authentification** des expéditeurs de messages,
  + **validation** des messages (contrôler que le message entrant contient un document XML en bonne et due forme et qu’il correspond à un schéma bien précis ou à un document WSDL décrivant le message),
  + **enrichissement** (« enrichment ») des messages (ajout de données à un message afin de le rendre plus utilisable et sensé pour un service ou une application spécifique),
  + **transformation** des messages (conversion du message au format visé),
  + **routage** du message sur la base du contenu,
  + **journalisation** (« logging ») des messages et du trafic des messages.
* Le FSB **accroît les possibilités de contrôle et de gouvernance**.

BOSA DT a établi un programme de gouvernance fixant d’une part les règles de conception des services FSB et (dans une moindre mesure) des services SA, et d’autre part les règles de connexion au FSB.

Cette connexion au FSB se fait par le biais d’un processus structuré, éprouvé et optimalisé afin de simplifier la complexité technologique et d'accroître ainsi la fiabilité de l’intercommunication.

Par ailleurs, le programme élabore des règles de collaboration entre *source authentique/service provider* et *utilisateur/service consumer* qui, après négociations, sont fixées dans un *Service Level Agreement (SLA)*.

Enfin, le programme définit l’ensemble des changements et des étapes de contrôle intégrés concernant le développement d’un service FSB (de la demande de modification à la production).

## Utilisation du service

### Plan pas à pas pour la connexion à un service FSB

Avant de pouvoir utiliser un service FSB, le candidat-utilisateur doit suivre les étapes suivantes :

1/ Sélection et documentation de services web

Les liens suivants vous conduiront vers les services web actuellement proposés sur le FSB. Chaque service est documenté et accompagné d’un guide détaillé à l’attention des utilisateurs : <http://dtservices.bosa.be/fr/services/fsb/catalogue>

2/ Enregistrement de votre demande auprès du Service Desk de BOSA DT

Vous devez soumettre une demande au Service Desk de BOSA DT afin de pouvoir utiliser un service web FSB spécifique.

Ceci est possible via le formulaire de contact en ligne à l'adresse suivante: <http://dtservices.bosa.be/fr/Contact>

Vous recevrez ensuite les deux types de documents suivants :

3/ AARF (*Administration Access Request Form*)

Demande d’autorisation et d’accès au *service provider*/à la source authentique.

En fonction du *service provider*, vous recevrez des liens vers les modèles de document (*templates*) à compléter.

Remarque : pour une demande de connexion à certaines sources authentiques comme le Registre national et le Registre Bis, vous devez non seulement introduire une demande d’accès mais aussi disposer au préalable d’une autorisation au chambre compétente du Comité de Sécurité de l’Information (CSI). Vous pouvez trouver plus d'informations à ce sujet sur : <https://dt.bosa.be/fr/csi>

Dans le cas contraire, la source authentique rejettera votre demande d’accès.

4/ TCRF (*Technical Connection Request Form*)

Collecte des données du *consumer* pour la configuration de la connexion à l’environnement de test et de production du FSB (adresses IP, contacts, consommation, certificats, etc.).

Nous recommandons de remplir dans le même document, si possible, les données de test et de production. Cela réduira considérablement la période ultérieure de mise en production.

5/ Négociation SLA & *capacity check*

Parallèlement à l’étape 6 et sur la base des infos que vous aurez fournies dans le TCRF, un SLA sera défini.

6/ Tests d’intégration (parallèlement à l’étape 5)

Après concertation et sur la base d’un planning validé mutuellement, vous bénéficierez d’un accès à l’environnement INT du FSB, sur lequel vous pourrez effectuer les tests nécessaires.

7/ Passage en production

Après concertation et sur la base d’un planning validé mutuellement, vous aurez accès à l’environnement PR du FSB.

### Rôles et responsabilités

Les services FSB donnent accès à des données. Ces dernières doivent être utilisées exclusivement par les utilisateurs et sous leur responsabilité exclusive dans les limites de la loi, de l’AR ou de l’autorisation du comité sectoriel dont ils disposent. Cela signifie notamment que les mesures nécessaires seront prises pour veiller à ce que seules les personnes compétentes puissent utiliser les données. Pour le traitement de données à caractère personnel, la loi relative à la protection de la vie privée doit à tout moment être respectée. En d’autres termes, cela signifie que les données ne peuvent être utilisées qu’aux fins préétablies et que le principe de proportionnalité doit être respecté.

Si les utilisateurs doutent de l’exactitude des données de la source authentique, ils ont l’obligation de le signaler à BOSA DT ou aux responsables de la source authentique, qui a ensuite elle-même le devoir d’examiner sérieusement la situation et de procéder aux corrections nécessaires éventuelles.

Les responsables des sources authentiques sont responsables des informations reprises dans ces sources selon la législation applicable. Ils s’engagent à organiser les processus de manière transparente afin de veiller à ce que les données soient aussi complètes, correctes, précises et à jour que possible.

BOSA DT s’engage à ce que la consultation des sources authentiques par les utilisateurs et la mise à disposition des données à ces derniers se déroulent comme décrit dans le *Catalogue FSB*.

BOSA DT s’engage à examiner, à chaque requête de consultation ou de communication, si l’utilisateur-demandeur et ladite requête satisfont aux règles de la source authentique, telles que définies dans la banque de règles adéquate (autorisation, gestion de l’identité et de l’accès, …).

Toutes les Parties s’engagent à prendre les mesures techniques et organisationnelles nécessaires pour protéger les données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé.

### Coûts liés à l’utilisation du service

L’utilisation du FSB de BOSA DT est gratuite. Cependant, des frais peuvent éventuellement être imputés au gestionnaire de la source authentique (c’est par exemple le cas pour le Registre national – plus d’infos sur le site web).

## Sécurité

### Sécurisation du FSB

BOSA DT assure une sécurisation optimale de l’accès au FSB et aux différents service providers.

L’accès au FSB est ouvert manuellement après un contrôle détaillé du Technical Connection Request Form complété par le service consumer. Seules les demandes signées remplies correctement et complètement sont traitées.

Pour la connexion réseau, des flux de firewall spécifiques sont ouverts et un certificat SSL est utilisé.

Au niveau de l’application, on utilise un certificat, le CN (Common Name) étant l’identificateur unique de l’application du service consumer. Un certificat existant ne peut être utilisé pour une seconde connexion FSB que moyennant l’accord de BOSA DT.

### Sécurisation de l’utilisateur final

BOSA DT règle via le FSB la sécurité de la connexion de l’application de l’utilisateur à la source authentique.

La sécurité et le contrôle d’accès des utilisateurs finaux doivent être assurés par l’utilisateur en personne. L’utilisateur se charge de bien sécuriser sa propre application et de mettre en place un système d’authentification des utilisateurs finaux.

L’utilisateur est conscient qu’il a peut-être affaire à des informations confidentielles, ce qui l’oblige à les traiter en tant que telles et à respecter la législation applicable.

Dans ce cadre, il ne peut notamment pas transmettre ces informations à des tiers sans autorisation spécifique.

### Finalité

La convention d'utilisation est conclue pour un service bien déterminé, et ce, dans un but (« finalité ») bien défini. Pour chaque nouvelle finalité, il convient de conclure une nouvelle convention d'utilisation et éventuellement de toujours demander une nouvelle autorisation.

L’utilisateur s’engage dès lors à ne faire usage que d’un accès bien précis dans le but spécifique lié à cet accès.

### Audittrail

L’utilisateur reconnaît que l’installation d’un audit trail est nécessaire dans le cadre du FSB. Cet audit trail assure que les transactions effectuées via le FSB puissent être reconstituées afin de respecter l’obligation légale (article 16 §4 de la loi du 8 décembre 1992) de sécuriser suffisamment les données à caractère personnel traitées via le FSB.

L’utilisateur reconnaît que le principe des « cercles de confiance » (circles of trust) s’appliquera au FSB. À cette fin, chaque partenaire de la chaîne sera tenu de prendre les mesures nécessaires pour conserver des données sélectionnées dans son audit trail, de manière à ce qu'il soit possible, par la combinaison des données tenues à jour par les différents partenaires de la chaîne, de parvenir à une reconstitution complète de l'ensemble du flux de données d'une transaction spécifique.

L’utilisateur reconnaît que d’autres partenaires de la chaîne dépendent, pour la reconstitution, des données qu’il tient à jour.

Dans le cadre d’un audit trail, l’utilisateur doit, pour un messageID et timestamp FSB fourni par BOSA DT, pouvoir indiquer qui est l’utilisateur final qui a lancé cette requête. Ces données doivent rester disponibles pendant 10 ans. Elles doivent pouvoir être fournies sur demande dans un délai de 24h.

L’utilisateur choisit lui-même les procédures et l’infrastructure permettant d’y arriver de manière sécurisée et dans le respect de la vie privée.

# Niveaux de service

# 

## Disponibilité

### Disponibilité du service

* Valeur cible dans l’environnement de production

Pour la plateforme FSB à proprement dite, un SLA a été conclu avec le prestataire de services de BOSA DT afin de garantir une disponibilité élevée.

99,95% pendant les heures d’activité et 99,5% en dehors de ces heures

Les heures d’activité s’étendent de 7h à 23h compris pendant les jours de la semaine sauf les jours fériés officiels.

La disponibilité des services web sur le FSB dépend cependant aussi du SLA conclu avec la source authentique.

BOSA DT utilisera tous les moyens raisonnables pour garantir une disponibilité aussi élevée que possible des services web.

* FSB dans l’environnement de production

Le FSB dans l’environnement de production est en principe disponible 24 heures sur 24 et 7 jours sur 7 (sauf fenêtres de maintenance planifiées). La fenêtre de support s’étend cependant de 9h à 17h en semaine (sauf jours fériés).

* FSB dans l’environnement d’intégration

Le service web dans l’environnement d’intégration est en principe disponible 24 heures sur 24 et 7 jours sur 7 (sauf fenêtres de maintenance planifiées). La fenêtre de support s’étend cependant de 9h à 17h en semaine (sauf jours fériés).

* Tests dans l’environnement d’intégration

Pour la réalisation de tests dans l’environnement d’intégration, le *service consumer* demandera une fenêtre de test au *service manager* de BOSA DT, sur présentation du plan de test. Cette procédure permet d’éviter la réalisation simultanée de tests par un nombre trop élevé de parties interférant entre elles.

**Procédure de réservation** : *meeting request* à [FSB-Integration@bosa.fgov.be](mailto:FSB-Integration@bosa.fgov.be), en mentionnant le numéro de téléphone du demandeur + le type de tests à réaliser.

* Procédure de *release*

BOSA DT prévoit 2 versions par service web au même moment. L’utilisateur s’engage à suivre le planning de *release* de BOSA DT et, si nécessaire, à passer à une nouvelle version, et donc aussi à refaire les tests et à prévoir les moyens nécessaires à cette fin, en cas d’installation d’une troisième version. Le nombre de nouvelles versions (avec impact) par an sera limité à 4 maximum.

Le *release* d’un changement ayant un impact sur le *service consumer* comprend 3 étapes :

* communication au sujet du planning du changement (conformément à la matrice ci-dessous) ;
* le changement est disponible dans l’environnement d’intégration (période de transition) ;
* le changement est mis en production.
* Documentation & gestion des versions

Toute la documentation sur chaque version d’un service web présent dans l’environnement d’intégration ou de production du FSB peut être librement consultée sur :  
<http://registry.fsb.belgium.be> (environnement PR)

* Exemple de matrice de changement (*change matrix*)

| **Type de changement** | **Changement majeur** |
| --- | --- |
| *Change backwards compatible* | 4 semaines à l’avance |
| *Change non backwards compatible* | 2 mois à l’avance |

Deux certificats sont utilisés dans l’environnement FSB :

* Remplacement du certificat de l’utilisateur

Le *service consumer* est responsable du suivi des certificats qu’il utilise. Il informera BOSA DT au moins 2 semaines à l’avance de la nécessité de remplacer un certificat. Pour des raisons de sécurité, la prolongation du certificat n’est pas autorisée.

* Renouvellement du certificat SSL du FSB

Le certificat FSB est renouvelé une fois par an. Les utilisateurs et responsables des sources authentiques recevront au moins 2 semaines à l'avance ce nouveau certificat et seront avertis, dans les mêmes délais, du moment exact de ce renouvellement.

### Capacité et performance

* Valeur cible

Pour la plateforme FSB à proprement dite, un SLA a été conclu avec le prestataire de services de BOSA DT afin de garantir une performance élevée.

La capacité et la performance des services web sur le FSB dépendent cependant aussi du SLA conclu avec la source authentique.

BOSA DT utilisera tous les moyens raisonnables pour garantir une performance aussi élevée que possible des services web.

* Utilisation des ressources

A la demande du *service provider*, il est possible d’imposer sur le FSB un nombre maximum de messages que l’utilisateur peut envoyer à la source authentique par unité de temps.

* Gestion de la capacité

Dans le cadre de la gestion de la capacité (capacity management) de BOSA DT, l’utilisateur informera BOSA DT de toute modification au volume prévu à l’origine qui est généré par l’utilisateur.

## Niveaux de service

Les niveaux de service seront convenus dans des SLA à signer individuellement (par famille de services web).

## Support

* *Incident flow*

Tous les incidents et questions sont initialement signalés au SD BOSA DT, qui transférera les appels aux personnes ou services adéquats au sein de BOSA DT.

* Priorités des incidents :

|  |  |
| --- | --- |
|  | **Description et critères** |
| **Priorité 1** | **Incident majeur** (Major Incident) – impact important sur le processus de travail. Le service est indisponible pour tous les utilisateurs.  Blocage du service ou erreur de fonctionnement du service touchant tous les utilisateurs ; la forte diminution de la performance rend le service inutilisable. Aucune solution de contournement (*workaround*) pour les activités n’est disponible. |
| **Priorité 2** | **Priorité élevée** (High Priority) – Incident bloquant ou grave.  Incidents ayant un impact sensible sur une partie du service. Aucune solution de contournement (workaround) pour les activités n’est disponible. |
| **Priorité 3** | **Priorité moyenne** (Medium Priority) – Incident sans gravité et sans impact sur les fonctions opérationnelles du service.  Le service ne fonctionne pas conformément aux spécifications mais l’impact sur les activités est minime ou une solution de contournement (*workaround*) utilisable est disponible. Tous les incidents relatifs aux activités qui ne sont pas une P1 ou P2 ou qui ne concernent pas un seul utilisateur. |
| **Priorité 4** | **Priorité normale** (Normal Priority) – Incident mineur ou requête de service, impact sur un seul utilisateur des activités.  Pas d’impact sur les activités ou problème fonctionnel mineur. Tous les tickets relatifs à des requêtes ou des plaintes ayant trait aux activités. |
| **Priorité 5** | **Priorité faible** (Low Priority) – Requêtes, questions ou service nécessaire pour un seul utilisateur final.  Tous les incidents ou requêtes de service des citoyens (pas d’impact sur les activités) |

* Matrice des priorités :

**Matrice d'urgence/d'impact pour les décisions relatives à la priorité accordée aux incidents en cas de doute :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Matrice des priorités** | | **IMPACT SUR LES ACTIVITES (business impact)** | | | |
| **Critique (Critical)** | **Sérieux (Serious)** | **Moyen (Medium)** | **Faible**  **(Low)** |
| **URGENCE** | **Critique (Critical)** | priorité1 | priorité1 | priorité2 | priorité2 |
| **Élevée (High)** | priorité1 | priorité2 | priorité2 | priorité2 |
| **Moyenne (Medium)** | priorité2 | priorité2 | priorité3 | priorité3 |
| **Faible (Low)** | priorité2 | priorité2 | priorité3 | priorité4 |
| **Requêtes (Requests)** | priorité4 | priorité4 | priorité5 | priorité5 |

**Définitions de l'impact sur les activités :**

**Critique** (Critical) – Impact sur un département tout entier ou délai de livraison/service critique ou impact élevé sur les activités sans solution de contournement (« workaround ») possible pour les activités

* **Sérieux** (Serious) – Un grand groupe d’utilisateurs est touché ou impact moyen sur les activités sans solution de contournement (« workaround ») possible pour les activités
* **Moyen** (Medium) – Un groupe spécifique ou plusieurs utilisateurs sont touchés ou faible impact sur les activités
* **Faible** (Low) – Un seul utilisateur est touché

**Définitions de l'urgence**

* **Critique** (Critical) – Incident majeur à traiter en priorité, en situation de gestion de crise
* **Elevée** (High) – Incident très urgent à traiter le plus rapidement possible
* **Moyenne** (Medium) – Incident urgent à traiter rapidement
* **Faible** (Low) – Incident non urgent
* **Requête** (Request) – Requête non urgente
* Délais de réaction :
  + La journalisation et le transfert de l’appel interviennent dans les 30 minutes.
  + Le feed-back des incidents intervient :
    - toutes les 2 heures de travail pour les incidents de classe 1
    - toutes les 4 heures de travail pour les incidents de classe 2
    - toutes les 12 heures de travail pour les incidents de classe 3
  + La remontée de l’incident vers le *service manager* intervient, si l’incident n’est pas encore résolu :
    - après 5 heures de travail pour les incidents de classe 1
    - après 12 heures de travail pour les incidents de classe 2
    - après 1 semaine pour les incidents de classe 3
  + L’e-mail initial du service web est journalisé et transféré dans un délai de 4 heures.
* Personnes de contact (exemple de tableau relatif aux personnes de contact)

| **Type de contact** | **Contact BOSA DT**  *(nom-fonction/tél.-GSM/e-mail/disponibilité)* | **Contact *service consumer***  *(nom-fonction/tél.-GSM/e-mail/disponibilité)* |
| --- | --- | --- |
| Single point of contact (SPOC) | SD BOSA DT  Via le formulaire de contact :  <http://dtservices.bosa.be/fr/Contact>  Par téléphone entre 8h30 et 17h les jours ouvrables de l'Administration fédérale :  02 740 79 94 (FR) 02 740 79 93 (NL) |  |
| Notification des incidents/questions | SD BOSA DT |  |
| Notification des changements/maintenance | SD BOSA DT |  |
| Escalade | Service Manager FSB |  |
| Remplaçant Escalade | Service Support FSB |  |
| Escalade + 1 | Domain Service Manager DIS |  |
| Statistiques d’utilisation | Service Manager FSB |  |
| Réunion de service | Service Manager FSB |  |

## Rapports et evaluation

S’il le souhaite, BOSA DT peut, à chaque trimestre, envoyer au service level manager du service consumer un rapport contenant les statistiques d’utilisation.

Par ailleurs, des réunions de service sont prévues pour assurer le suivi des niveaux de service, parcourir les incidents majeurs et discuter des anciens et nouveaux changements. La fréquence de ces réunions sera convenue de commun accord entre BOSA DT et le service consumer.

## Modification des niveaux de service

Chaque année est organisée une review meeting entre les service managers de BOSA DT et de l’utilisateur afin d’examiner et éventuellement adapter le SLA.

# Parties et signature

Le service est offert à l'utilisateur par le Service public fédéral Technologie de l'Information et de la Communication (« BOSA DT »).

L'utilisation du service est soumise aux conditions générales, à la présente convention d'utilisation, en ce compris le Service Level Agreement (SLA), ainsi qu'aux directives techniques et autres de BOSA DT concernant le service.

En signant la présente convention d'utilisation, l'utilisateur se déclare d'accord avec les conditions générales relatives aux services de BOSA DT.

|  |  |  |
| --- | --- | --- |
|  | Utilisateur du service | Fournisseur du service |
| *Nom de l’organisation :*  *Nom du signataire :*  *Fonction du signataire :* |  | SPF BOSA DG DT  Jack Hamande  Directeur-Général |
| *Date de la signature :*  *Signature :* |  |  |

Annexe: Conditions générales liées aux services du SPF BOSA DG DT. La version la plus récente peut-être retrouvée au: <https://dt.bosa.be/fr/echange_de_donnees>