FOD Beleid & Ondersteuning
SPF Stratégie & Appui

Convention d'utilisation FAS

Organisation:
Application:

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 la DG SD du SPF BOSA. 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 la DG SD du SPF BOSA.

Veuillez également toujours utiliser la dernière version de ce document à ce lien

1. Conditions spécifiques 3
1.1 DESCRIPTION ET FONCTIONNEMENT DU SERVICE 3
Objet de la présente convention 3
Fonctionnement du service 3
1.2 DEMANDE D'ADHÉSION AU SERVICE 3
1.3 UTILISATION DU SERVICE 4
Conditions d'utilisation du service 4
Rôles et responsabilités liés au service 4
Traitement de données à caractère personnel 5
Coûts liés à l'utilisation du service 7
1.4 SÉCURITÉ 7
Sécurisation par l'utilisateur 7
Piste d'audit 7
2. Niveaux de service 8
2.1 CHAMP D'APPLICATION DE CES NIVEAUX DE SERVICE 8
Ne font pas partie des niveaux de service : 9
2.2 DISPONIBILITÉ 9
Indisponibilité planifiée 9
2.3 CLASSIFICATION DES INCIDENTS 9
2.4 SUPPORT 10
Support 10
Délégué à la protection des données 10
Support complémentaire 10
2.5 INFORMATIONS, RAPPORTS ET ÉVALUATION 10
Informations 10
Monitoring 10
Rapports 11
3. Parties et signature 11

1. Conditions spécifiques

1.1 DESCRIPTION ET FONCTIONNEMENT DU SERVICE

Objet de la présente convention

La DG Simplification et Digitalisation du Service public fédéral Stratégie et Appui (DG SD du SPF BOSA) offre le service d'authentification fédéral conformément à l'article 9 de la loi du 18 juillet 2017 relative à l'identification électronique. Le Federal Authentication Service (FAS) permet aux utilisateurs d'authentifier des personnes (utilisateurs finaux) de sorte qu'elles puissent accéder à des applications publiques en ligne sécurisées.

Les applications publiques en ligne sont des applications qui appartiennent à des instances publiques, à des instances ayant une mission d'intérêt général pour leurs missions d'intérêt général et à des instances qui exécutent une mission pour le compte des instances publiques et des instances ayant une mission d'intérêt général. L'utilisateur reconnaît appartenir à ces catégories d'instances.

Fonctionnement du service

Le FAS a été conçu pour contrôler les données d'authentification d'un utilisateur final.
Un utilisateur final qui se connecte à une application publique en ligne sera dirigé par le FAS vers le portail fédéral d'authentification de la DG SD du SPF BOSA.

Le FAS offrira à l'utilisateur final un écran pour s'enregistrer et lui demandera les données nécessaires. Après réception des données d'authentification, le FAS reconduit l'utilisateur final vers l'application en ligne, en même temps que le message de réponse. Ce dernier contient les informations d'authentification. L'application publique en ligne réceptrice de l'utilisateur peut, sur la base de ce message de réponse, prendre la décision de donner accès à l'utilisateur final.
C'est l'utilisateur lui-même qui décide donc si un utilisateur final a le droit ou non de bénéficier de l'accès (autorisation) ; le FAS garantit quant à lui à cet utilisateur que la personne est bien celle qu'elle prétend être. Les décisions d'autorisation (droits d'accès à l'application en ligne) continuent donc à incomber à l'utilisateur.

Le FAS comprend différents moyens d'authentification ou clés numériques, qui sont utilisés en fonction de la sensibilité des informations, notamment :

- Nom d'utilisateur et mot de passe
- Nom d'utilisateur et mot de passe, et code de sécurité unique limité dans le temps via application mobile
- Nom d'utilisateur et mot de passe et certificat numérique personnel
- Nom d'utilisateur et mot de passe, et code de sécurité unique limité dans le temps par SMS
- Nom d'utilisateur et mot de passe, et code de sécurité unique limité dans le temps par e-mail
- Carte d'identité électronique avec code PIN + lecteur de cartes
- « Moyen d'identification électronique agréé » ; itsme® et myID.be®
- Identification électronique reconnue au plan européen (eIDAS)

1.2 DEMANDE D'ADHÉSION AU SERVICE

La demande d'adhésion au service FAS se concrétise par la rédaction d'un document d'onboarding. Ce dernier est annexé à la présente convention. Ce document contient des accords conclus avec l'utilisateur concernant les aspects techniques et relatifs à la gestion des services.

Toute proposition d'adaptation de ces accords doit être demandée au minimum un trimestre à l'avance. La DG SD du SPF BOSA évaluera chaque proposition, informera l'utilisateur en temps utile des suites concrètes éventuellement données à la proposition, et communiquera un timing. La modification approuvée sera ensuite annexée à la présente convention.

1.3 UTILISATION DU SERVICE

Conditions d'utilisation du service

L'utilisateur prend les mesures organisationnelles et techniques nécessaires pour veiller à ce que le FAS soit utilisé et implémenté conformément à la présente convention d'utilisation, aux directives de la DG SD du SPF BOSA contenues dans les formulaires et guides techniques de l'onboarding et à la législation applicable.

Vous ne pouvez pas utiliser le FAS d'une manière qui pourrait désactiver, surcharger ou altérer ce service ou affecter négativement l'expérience utilisateur d'un autre utilisateur.

Les tests et la surveillance (monitoring) dans l'environnement de production du FAS ne sont pas autorisés si ce n'est à titre exceptionnel et moyennant l'accord écrit et explicite de la DG SD du SPF BOSA.

Les directives de la DG SD du SPF BOSA peuvent imposer une migration du FAS existant vers une nouvelle version de celui-ci. Dans ce cas, sauf convention contraire avec la DG SD du SPF BOSA, l'utilisateur dispose d'une période de 6 mois à partir de la mise à disposition du nouveau service pour procéder à son implémentation. Au-delà de cette période, la DG SD du SPF BOSA n'est plus tenue de mettre à disposition des anciennes versions ni d'assurer leur maintenance.

Rôles et responsabilités liés au service

Il incombe à l'utilisateur de veiller à ce que son application :

- o interprète correctement la réponse du FAS :
- o soit suffisamment sécurisée ;
- o valide les certificats de manière correcte ;
- o implémente le « Single Log Out » (SLO) correctement, si elle utilise un « Single Sign On » (SSO) ;
- o donne accès aux services à l'utilisateur final ou à une partie de ceux-ci, en fonction des règles d'accès définies par l'utilisateur lui-même.

L'utilisateur est personnellement responsable du contenu des services auxquels il donne accès ainsi que de la définition des règles d'accès aux services et du niveau des moyens d'authentification nécessaire pour accéder à ces services. L'utilisateur est averti que les niveaux de sécurisation diffèrent selon les moyens d'authentification. Ainsi, la combinaison nom d'utilisateur/mot de passe n'est pas un moyen d'authentification fortement sécurisé et elle ne doit dès lors être utilisée que lorsque le niveau de sécurisation requis n'est pas élevé. La carte d'identité électronique est quant à elle un moyen d'authentification fortement sécurisé.

L'utilisateur déclare être conscient du fait que la sécurisation des ordinateurs sur lesquels l'application est implémentée ainsi que la sécurisation des mots de passe sont des éléments importants de la sécurité fonctionnelle du système. Le manque de sécurisation de l'environnement de l'utilisateur ou de l'utilisateur final peut donc avoir une influence sur le fonctionnement du système. La DG SD du SPF BOSA ne peut cependant assumer aucune responsabilité pour ce qui est de la sécurisation de l'environnement de l'utilisateur ou de l'utilisateur final dans la mesure où elle n'a pas le moindre contrôle sur celui-ci.

Si l'utilisateur fait appel à un sous-traitant, il est entièrement responsable du respect par le sous-traitant des obligations de l'utilisateur dans le cadre de la présente convention.

La DG SD du SPF BOSA vise à mettre le service à disposition selon les niveaux de service définis au point 2 sans pouvoir donner de garanties en la matière. La DG SD du SPF BOSA dépend partiellement des niveaux de service offerts par les sources authentiques appelées par le FAS.

La DG SD du SPF BOSA est responsable de l'acheminement du message de demande vers la source authentique appropriée et du renvoi à l'utilisateur de la réponse basée sur les données de la source authentique.

Les gestionnaires des sources authentiques sont responsables des informations contenues dans ces sources conformément à la législation applicable.

Lorsque les utilisateurs doutent de la justesse des données contenues dans la source authentique, ils sont tenus d'en informer la DG SD du SPF BOSA ou les responsables de la source authentique. La source authentique est ensuite tenue d'analyser sérieusement l'information et, le cas échéant, d'apporter les corrections nécessaires.

Traitement de données à caractère personnel

Le traitement par la DG SD du SPF BOSA des données des utilisateurs finaux pendant l'enregistrement et pendant l'utilisation des clés numériques est justifié sur la base de l'article 9 de la loi du 18 juillet 2017 relative à l'identification électronique, qui charge la DG SD du SPF BOSA d'offrir des clés numériques pour des applications des autorités au sein du FAS. Il s'agit aussi de la base pour le traitement du numéro de Registre national par la DG SD du SPF BOSA au sein du FAS.
Les données sont traitées en vue de l'identification et de l'authentification correctes des utilisateurs finaux afin que les utilisateurs puissent prendre une décision au sujet de l'accès aux applications.

Pour l'enregistrement initial, le FAS utilise la carte d'identité électronique, et plus précisément son certificat d'authentification, les nom et prénom tels que mentionnés sur la carte, ainsi que le numéro de Registre national.
Une autre façon d'enregistrer initialement des utilisateurs finaux est de passer par un bureau d'enregistrement.

Pour l'activation de certaines clés, l'utilisateur final doit introduire l'adresse e-mail et le numéro de GSM. Pour la création de certaines clés, les sources authentiques du Registre national ou des registres de la Banque Carrefour de la BCSS (Registre Bis) sont consultées.

En cas d'authentification de l'utilisateur final par le biais du FAS, le numéro de Registre national est transmis à l'application publique en ligne à laquelle l'utilisateur final demande d'accéder.

Les utilisateurs doivent être autorisés à utiliser le numéro de Registre national pour l'identification et l'authentification. S'ils n'y sont pas autorisés, un autre numéro d'identification peut être utilisé pour l'identification et l'authentification.

Pour l'authentification via eIDAS (à travers les frontières des États membres européens) basée sur le règlement eIDAS, la DG SD du SPF BOSA récupère les données dans le Registre national pour les fournir à l'État membre dans lequel l'utilisateur final se connecte avec une clé numérique notifiée en Belgique. Il s'agit de la date de naissance, des nom et prénom, ainsi que d'un numéro d'identification destiné à l'authentification transfrontalière. La base légale à cette fin est l'article 5 de la loi du 18 juillet 2017 relative

à l'identification électronique et l'Arrêté royal du 1er février 2018 désignant des instances conformément à la loi du 18 juillet 2017 relative à l'identification électronique.

Avec l'accord de l'utilisateur final, la DG SD du SPF BOSA traite aussi l'adresse e-mail et/ou le numéro de GSM pour contacter l'utilisateur final au sujet des services. Ces données sont alors utilisées pour envoyer des notifications de services liées aux services fournis.

Les authentifications et tentatives d'authentification (date, heure, numéro d'identification et identification du message afin qu'il puisse être relié à l'application, à l'adresse IP, au navigateur et au système d'exploitation) sont enregistrées et stockées dans une piste d'audit afin qu'en cas d'enquête, à l'initiative d'une instance compétente ou d'un organe de contrôle ou à la suite d'une plainte, il soit possible de reconstituer complètement quelle personne physique s'est enregistrée auprès de quel service et quand. Ces informations sont conservées pendant 10 ans.

Ces informations sont également traitées de manière anonymisée à des fins statistiques et afin de continuer à améliorer ce service. Les données ainsi collectées ne sont en aucun cas liées aux données à caractère personnel qui ont été collectées pendant la procédure d'enregistrement.
Les traitements (à l'exception de la conservation dans la piste d'audit) s'arrêteront lorsque l'utilisateur final cessera explicitement d'utiliser ses clés numériques au sein du FAS ou lorsqu'il décédera. Les données seront ensuite détruites.
Les données dans la piste d'audit seront supprimées après 10 ans.

Le FAS offre également des clés numériques de prestataires de services agréés.
Les prestataires de services agréés (comme les fournisseurs itsme® et myID.be®) traitent aussi les données conformément à la réglementation en vigueur. Après avoir été agréés conformément à l'Arrêté royal du 22 octobre 2017 fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques numériques, ils sont autorisés à utiliser le numéro de Registre national si l'utilisateur final choisit leurs services (en tant que sous-traitants de l'autorité d'agrément au sens de l'article 5, alinéa premier, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques).

Pour ces traitements, la DG SD du SPF BOSA agit en tant que responsable du traitement au sens de l'art. 4, 7° du RÈGLEMENT (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD »).

Pour le traitement des données dans son application publique en ligne, l'utilisateur agit en tant que responsable du traitement au sens de l'art. 4, 7° du RGPD. Il s'agit du traitement des données qu'il reçoit du FAS et qu'il traite pour le contrôle d'accès à l'application publique en ligne.
Cela signifie notamment que les mesures nécessaires seront prises pour garantir que seules les personnes compétentes peuvent utiliser les données, que les données ne peuvent être utilisées qu'aux fins préétablies et que le principe de proportionnalité doit être respecté.

Les données à caractère personnel des utilisateurs finaux que le FAS confirme à l'utilisateur dans le message de réponse sont uniquement destinées à la gestion des utilisateurs. Tout traitement de ces données autre que l'identification, l'authentification et l'autorisation de l'utilisateur final est proscrit. L'utilisateur ne peut dès lors utiliser ces données que pour vérifier le statut de la procédure d'authentification achevée et pour déterminer à quelles données l'utilisateur final peut accéder par le biais de l'application.

L'utilisateur ne peut conserver les données à caractère personnel contenues dans le message de réponse plus longtemps qu'il n'est nécessaire pour la finalité « gestion des utilisateurs ».

La DG SD du SPF BOSA et l'utilisateur s'aident mutuellement à s'acquitter de leur obligation de donner suite aux demandes dont les personnes concernées les saisissent en vue d'exercer leurs droits et à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD.

La DG SD du SPF BOSA et l'utilisateur tiennent à jour un registre des activités de traitement. Sur simple demande raisonnable, ils sont tenus de présenter ce registre.

Si la DG SD du SPF BOSA ou l'utilisateur prend connaissance d'une violation des données à caractère personnel mises à disposition, ils s'en informent mutuellement dans les meilleurs délais.

La DG SD du SPF BOSA et l'utilisateur s'engagent à respecter le RGPD ainsi que toute autre législation pertinente relative au traitement des données.
La DG SD du SPF BOSA et l'utilisateur s'engagent à informer les personnes agissant sous son autorité des dispositions du RGPD et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel.

Les deux Parties ont désigné un délégué à la protection des données et disposent d'une politique et d'un plan de sécurité actuels qui sont révisés annuellement.

Les deux 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 de données.
Les deux Parties s'engagent à documenter toutes les mesures.

Les responsables des sources authentiques sont les responsables du traitement au sens de l'art. 4, 7° du RGPD pour les données dans leurs propres sources authentiques. Ils sont responsables de l'organisation des processus de manière transparente pour faire en sorte que les données soient aussi complètes, exactes, précises et actualisées que possible. Ils sont responsables de la collecte des données dans la source authentique, de l'enregistrement des données avec des garanties de qualité et de disponibilité, et de la décision de mise à disposition.

Coûts liés à l'utilisation du service

L'utilisation de ce service est gratuite.

Le paiement éventuel dû aux responsables des sources authentiques pour les services de la source d'information est à charge de l'utilisateur qui recourt aux services de cette source authentique.

1.4 SÉCURITÉ

Sécurisation par l'utilisateur

La DG SD du SPF BOSA régit la sécurité de la connexion entre le FAS et l'application de l'utilisateur. Il incombe à l'utilisateur d'assurer une sécurisation adéquate de sa propre application et des données.

Piste d'audit

L'utilisateur reconnaît que la mise en place d'une piste d'audit (audit trail) est nécessaire dans le cadre du FAS. Cet audit trail assure que les transactions effectuées via le FAS puissent être reconstituées afin de respecter l'obligation légale de sécuriser suffisamment les données à caractère personnel traitées via le FAS.

L'utilisateur reconnaît que le principe des « cercles de confiance » (circles of trust) sera appliqué. De ce fait, chaque partenaire de la chaîne est tenu à titre individuel de prendre les mesures nécessaires pour conserver des données sélectionnées dans sa piste d'audit, 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 reconstruction complète de l'ensemble du flux de données d'une transaction spécifique.

L'utilisateur reconnaît que pour ladite reconstruction, d'autres partenaires de la chaîne dépendent des données qu'il tient lui-même à jour.

Dans le cadre d'une piste d'audit, l'utilisateur enregistre

- pour un SAML fourni par la DG SD du SPF BOSA :
  le messageID (SAML auth request ID / SAML response ID), le timestamp
- pour un OIDC fourni par la DG SD du SPF BOSA :
  le messageID (state), autorisation code, le timestamp

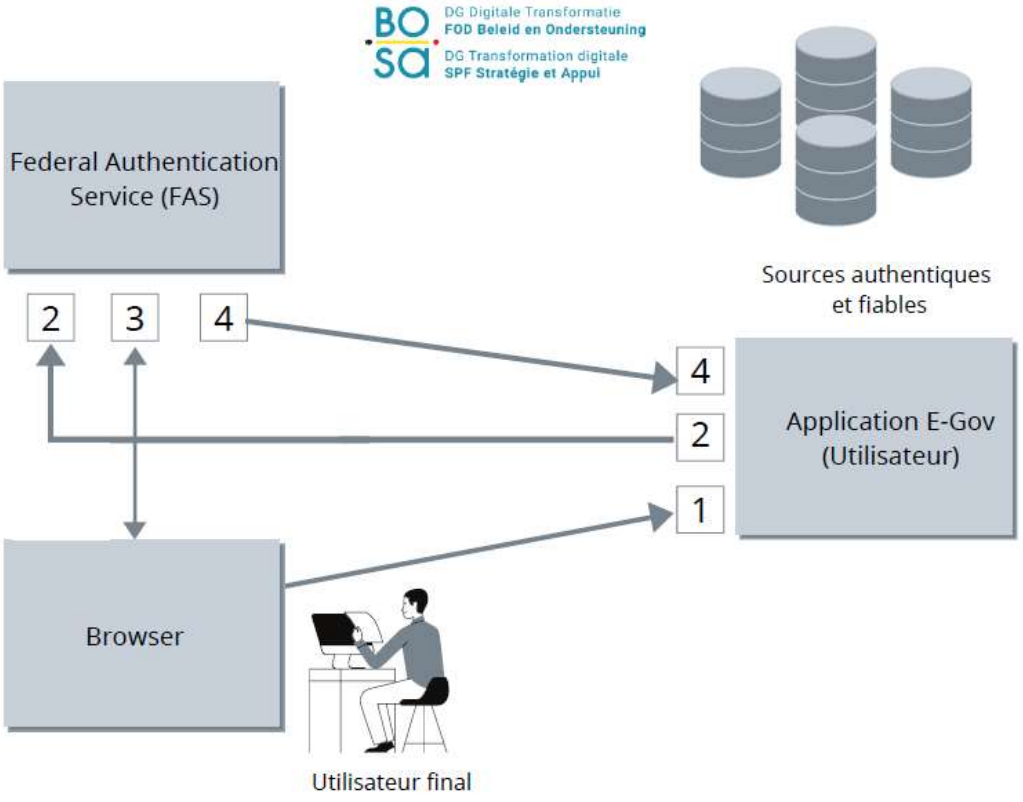
et l'utilisateur final y afférent, qui a initié cette demande.

Toutes les Parties veillent à ce que ces données restent disponibles pendant une période de 10 ans et à ce qu'elles puissent être fournies sur demande dans un délai de trois jours ouvrables.
L'utilisateur est lui-même responsable des procédures et de l'infrastructure qui lui permettront de répondre à ces exigences de manière sécurisée et dans le respect de la vie privée.

2. Niveaux de service

La DG SD du SPF BOSA fournira des efforts raisonnables pour respecter les objectifs de service ci-dessous.

2.1 CHAMP D'APPLICATION DE CES NIVEAUX DE SERVICE



Les systèmes et fonctionnalités gérés et utilisés par la DG SD du SPF BOSA pour l'utilisateur :

- Le traitement des demandes d'authentification émanant de l'utilisateur comme convenu dans le document d'« onboarding » établi avec l'utilisateur.

- L'échange de données d'authentification de la personne exécutant l'authentification :
  - FEDID
  - Numéro de Registre national
  - Prénom, Nom de famille
  - Date de naissance (eIDas)

Ne font pas partie des niveaux de service :

- Toutes les informations opérationnelles soutenant les services découlant de la présente convention ne font pas partie de cette dernière.
- Les systèmes et fonctionnalités non gérés et utilisés par la DG SD du SPF BOSA, que l'utilisateur utilise/possède pour offrir ses services à son utilisateur final.
- La configuration et le support de l'application de l'utilisateur qui fait l'objet de l'intégration au FAS (Relying Party).
- La configuration et le support de l'appareil de l'utilisateur final, en ce compris mais sans s'y limiter : le middleware eID, le navigateur, le système d'exploitation…
- La disponibilité des sources authentiques.
- Le SSO interne ou équivalent pour de l'interprocessus dans une application
- Des limitations fonctionnelles ou de développement d'une application

2.2 DISPONIBILITÉ

Le service FAS est disponible 24 heures sur 24 et 7 jours sur 7.

Indisponibilité planifiée

En cas d'indisponibilité planifiée, les clients sont prévenus par e-mail 1 semaine à l'avance. Cet e-mail contient la date, l'heure de début et la durée de l'interruption.

2.3 CLASSIFICATION DES INCIDENTS

Classification	Description de l'incident	Canal de notification
Priorité 1	Le service FAS est entièrement indisponible. *(Toutes les applications rencontrent des problèmes. 100 % d'indisponibilité)*	Téléphone, e-mail
Priorité 2	Le service FAS est partiellement indisponible. *(Certaines applications rencontrent des problèmes. Les utilisateurs de ces applications ne peuvent plus travailler.)*	Téléphone, e-mail
Priorité 3	Le service FAS est légèrement affecté. *(Certaines applications rencontrent des problèmes. Les utilisateurs peuvent encore travailler.)*	Téléphone, e-mail
Priorité 4	Demande informative	Téléphone, E-mail, Formulaire web

2.4 SUPPORT

L'ensemble des incidents et demandes sont d'abord notifiés au Service Desk de la DG SD du SPF BOSA. Ce dernier les transfère ensuite à la personne ou au service compétent au sein de la DG SD du SPF BOSA.

Support

Il est de la responsabilité de l'utilisateur d'offrir un support suffisant (de première ligne) aux utilisateurs finaux en termes d'équipements et de solidité pour les services qu'il propose personnellement. En aucun cas, sauf disposition contraire, le Service Desk de la DG SD du SPF BOSA ne fournira directement des services aux utilisateurs finaux de l'utilisateur.

Pour les utilisateurs (support de seconde ligne), le Service Desk de la DG SD du SPF BOSA est joignable :

- Par téléphone : 02 474 50 62
  entre 8h30 et 17h00 les jours ouvrables de l'Administration fédérale
- Par e-mail : Servicedesk.DTO@bosa.fgov.be

Délégué à la protection des données

Vous pouvez contacter le DPD de la DG SD du SPF BOSA par e-mail à privacy@bosa.fgov.be pour toutes vos questions relatives à la protection de la vie privée. Vous pouvez communiquer vos incidents et envoyer vos plaintes à privacyincident@bosa.fgov.be.

Support complémentaire

Pour plus d'informations ou pour utiliser le service, veuillez contacter le Service Desk de la DG SD du SPF BOSA par e-mail à Servicedesk.DTO@bosa.fgov.be en indiquant la référence « S001 – FAS ».

2.5 INFORMATIONS, RAPPORTS ET ÉVALUATION

Informations

La DG SD du SPF BOSA avertira les utilisateurs dans les cas suivants :

- **Interruption planifiée** : une modification nécessaire entraîne une interruption de service planifiée. Dans ce cas, la DG SD du SPF BOSA communiquera par e-mail au client la date et la période d'interruption.
- **Incidents** : un incident mène à une interruption de service. Le client sera informé de l'évolution de l'incident et de la restauration du service.
- **Modifications aux certificats** : le client sera averti à l'avance de l'échéance de son certificat et recevra les informations nécessaires pour le renouveler.
- **Nouvelles** : nouvelles relatives aux services.
- **Modifications contractuelles** : en cas d'adaptations aux conventions d'utilisation.

Afin de pouvoir fournir ces informations, l'utilisateur doit toujours transmettre à la DG SD du SPF BOSA les coordonnées les plus récentes.

Monitoring

L'utilisateur n'est pas autorisé à surveiller le FAS d'une manière susceptible d'influencer la performance du FAS. Cependant, la DG SD du SPF BOSA peut, sur demande, fournir à l'utilisateur un monitoring par le biais de fichiers et fichiers de journalisation (« log files ») Json.

Rapports

Rapports disponibles sur demande dans la limite de nos capacités et limités à une période antérieure d'un an.

3. Parties et signature

Le service est offert à l'utilisateur par la DG Simplification et Digitalisation du Service public fédéral Stratégie et Appui, Boulevard Simon Bolivar 30, 1000 Bruxelles.

L'utilisation du service est soumise aux conditions générales, à la présente convention d'utilisation ainsi qu'aux directives techniques et autres de la DG SD du SPF BOSA concernant le service.

En signant la présente convention d'utilisation, l'utilisateur se déclare d'accord avec les conditions générales des services de la DG SD du SPF BOSA.

Signé le date :

Nom de l'utilisateur :

Représentant de l'utilisateur :

Organisation :

Numéro BCE :

Fonction du représentant :

Signature :

Annexe 1 : Conditions générales des services de la DG SD du SPF BOSA

Les conditions générales sont publiées sur le site web de la DG SD du SPF BOSA :
https://bosa.belgium.be/fr/conditions-generales-services-dg-simplification-et-digitalisation