CONVENTION D'UTILISATION FAS

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 Fedict. 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 Fedict.

Statut : 3.0

Date : 25/09/2012

Fedict - Federale Overheidsdienst ICT
Fedict - Service Public Fédéral ICT

Table des matières

1. Conditions spécifiques

1.1. DESCRIPTION ET FONCTIONNEMENT DU SERVICE

1.1.1. Objet de la présente convention

Le *Federal Authentication Service* (FAS) permet aux utilisateurs d'enregistrer et d'authentifier des personnes (utilisateurs finaux) de sorte qu'elles puissent accéder à des applications en ligne sécurisées.

1.1.2. 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 en ligne sera dirigé par le FAS vers le portail fédéral d'authentification de Fedict. 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 reconduira 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 réceptrice de l'utilisateur peut, sur la base de ce message de réponse, prendre la décision d'ouvrir une session pour l'utilisateur final.

C'est l'utilisateur lui-même qui décide 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.

1.2. UTILISATION DU SERVICE

1.2.1. Conditions d'utilisation du service

Le test 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 Fedict.

Les directives de Fedict peuvent imposer une migration du FAS existant vers une nouvelle version de celui-ci. Dans ce cas, sauf convention contraire avec Fedict, 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, Fedict n'est plus tenu de mettre à disposition des anciennes versions ni d'assurer leur maintenance.

1.2.2. Rôles et responsabilités liés au service

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

- interprète correctement la réponse du FAS ;
- soit suffisamment sécurisée ;
- valide les certificats de manière correcte ;
- donne accès aux services de l'utilisateur ou à une partie de ceux-ci, en fonction des règles d'accès définies par l'utilisateur lui-même.

L'utilisateur est responsable du contenu des services auxquels il donne accès.

L'utilisateur déclare être conscient du fait que la sécurisation des ordinateurs sur lesquels l'application est déployée 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. Fedict 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 il 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.

Fedict est responsable de la mise à disposition du service conformément aux niveaux de service définis au point 2.

Fedict 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. Ils s'engagent à organiser les processus de manière transparente pour faire en sorte que les données soient aussi complètes, exactes, précises et actualisées que possible.

Lorsque les utilisateurs doutent de la justesse des données contenues dans la source authentique, ils sont alors tenus de le signaler à Fedict ou aux responsables de la source authentique. La source authentique est ensuite tenue d'analyser sérieusement la déclaration et, le cas échéant, d'apporter les corrections nécessaires.

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 de données.

1.2.3. Coûts liés à l'utilisation du service

L'utilisation de ce service est gratuite.

1.2.4. Autorisation du comité sectoriel

L'utilisateur confirme disposer d'un A.R. ou d'une autorisation du comité sectoriel du Registre national qui donne accès aux données du Registre national ou qui permet l'utilisation du numéro de Registre national pour la finalité « gestion des utilisateurs ». Le traitement des données relève de la responsabilité exclusive de l'utilisateur qui ne peut les traiter que selon les modalités prévues dans l'A.R. ou dans l'autorisation du comité sectoriel et selon les dispositions de la loi relative à la protection de la vie privée.

L'utilisateur confirme disposer d'un A.R. ou d'une autorisation du comité sectoriel compétent qui donne accès aux autres données d'authentification demandées pour la finalité « gestion des utilisateurs ». Le traitement des données relève de la responsabilité exclusive de l'utilisateur qui ne peut les traiter que selon les modalités prévues dans l'A.R. ou dans l'autorisation du comité sectoriel et selon les dispositions de la loi relative à la protection de la vie privée.

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.

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 ».

L'utilisateur prend les mesures organisationnelles et techniques nécessaires pour veiller à ce que le FAS soit utilisé et déployé conformément à la présente convention d'utilisation, aux directives de Fedict et à la législation applicable, en particulier celle relative à la protection de la vie privée. Cela signifie notamment que l'utilisateur prend toutes les mesures possibles pour garantir la sécurité et la confidentialité des données et pour prévenir les abus et les pertes de données.

1.3. SÉCURITÉ

1.3.1. Sécurisation de l'utilisateur

Fedict 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.

L'utilisateur est conscient qu'il manipule des données à caractère personnel, ce qui l'oblige à les sécuriser et à respecter la législation applicable en la matière.

1.3.2. « Audit Trail »

L'utilisateur reconnaît que la mise en place d'un *audit trail* est nécessaire dans le cadre du FAS. Cette piste de vérification fait en sorte que les transactions qui sont exécutées via le FAS peuvent être reconstruites aux fins de respecter l'obligation légale qui impose de sécuriser suffisamment les données à caractère personnel traitées via le FAS (article 16, §4, de la loi du 8 décembre 1992).

L'utilisateur reconnaît que le principe des « cercles de confiance » (*circles of trust*) sera appliqué. Il s'ensuit que chaque partenaire de la chaîne est tenu à titre individuel 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 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'un *audit trail*, l'utilisateur doit, pour un SAML fourni par Fedict, pouvoir livrer le messageID, le *timestamp* et l'utilisateur final, initiateur de la demande, y afférent.

Ces données doivent rester disponibles pendant une période de 10 ans.
Sur demande, ces données doivent pouvoir être fournies dans les 24 heures.

L'utilisateur choisit lui-même les procédures et 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

2.1. DISPONIBILITÉ

2.1.1. Disponibilité du service

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

2.1.2. 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.

2.1.3. Indisponibilité non planifiée

En cas d'indisponibilité non planifiée, les clients sont informés par e-mail de l'interruption. Dès que le service est à nouveau disponible, un e-mail est également envoyé pour annoncer la restauration de la disponibilité.

2.2. CLASSIFICATION DES INCIDENTS

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

2.3. NIVEAUX DE SERVICE

La prestation de services actuelle s'opère sur la base du « meilleur effort ».

2.4. SUPPORT

Tous les incidents et demandes sont d'abord notifiés au Service Desk de Fedict. Ce dernier les transfère ensuite à la personne ou au service compétent au sein de Fedict.

2.4.1. Support de première ligne

Le Service Desk de Fedict intervient en tant que point de contact unique.

Il est joignable :

- par téléphone entre 8h et 18h les jours ouvrables de l'administration fédérale
  au 078 15 03 13 pour les appels de type « business »
  au 078 15 03 11 pour les appels de type « citizen » (citoyens)
- par e-mail (disponibilité permanente) : servicedesk@fedict.belgium.be
- par formulaire web, disponible en permanence : www.fedict.belgium.be

2.4.2. Support supplémentaire

Pour plus d'informations ou pour utiliser le service, vous pouvez contacter le Service Desk de Fedict à l'adresse servicedesk@fedict.belgium.be en mentionnant la référence « S001 – FAS ».

2.5. RAPPORTS ET ÉVALUATION

2.5.1. Surveillance (monitoring)

Il n'est pas permis à l'utilisateur de surveiller le FAS d'une manière susceptible d'influencer la performance du FAS. Sur demande, Fedict peut cependant fournir des fichiers de journalisation (*log files*) à l'utilisateur.

2.5.2. Rapports

Aucun rapport SLA n'est disponible.

3. Parties et signature

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

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

En signant la présente convention d'utilisation, l'utilisateur se déclare d'accord avec les conditions générales des services de Fedict.

Signé le date

Nom de l'utilisateur
Représentant de l'utilisateur

Signature

Annexe 1 : Conditions générales relatives aux services de Fedict
Annexe 2 : Autorisations
Annexe 3 : Coordonnées

Annexe 1 : Conditions générales relatives aux services de Fedict

Les conditions générales sont reprises dans un document distinct qui se trouve sur le site web de Fedict :

http://www.fedict.belgium.be/fr/binaries/Algemene%20voorwaarden_%20Fedict%20diensten_2%207_FR_24112010_tcm461-131716.pdf

Annexe 2 : Autorisations

Le soussigné confirme :

- disposer de l'autorisation/des autorisations nécessaire(s) conformément à l'article 1.2.4 de la présente convention d'utilisation ;
- mentionner ci-dessous la/les référence(s) de l'autorisation/des autorisations[1] ;
- joindre une copie de l'autorisation si elle n'est pas déterminée dans une loi ou un A.R.

Nom et prénom

Organisation

Date

Signature

[1] Exemple : Arrêté royal du 30/08/1985 autorisant les administrations communales à utiliser le numéro d'identification du Registre national des personnes physiques ; Dossier numéro 1985-08-30/40 ; entrée en vigueur 27-09-1985

Annexe 3 : Coordonnées

Le but de cette annexe est de rassembler les coordonnées afin que Fedict puisse informer ses clients des services qu'il fournit.

Fedict avertira les utilisateurs dans les cas suivants :

- **Interruption planifiée** : une modification nécessaire entraîne une interruption de service planifiée. Dans ce cas, Fedict 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 des certificats** : le client sera averti à l'avance de l'échéance de son certificat et recevra les informations nécessaires pour le renouveler.
- **Actualités** : nouvelles relatives aux services.
- **Modifications des contrats** : en cas d'adaptations aux conventions d'utilisation et/ou SLA.
- **Rapports** : rapports sur les services utilisés.

Pour pouvoir fournir ces informations à ses clients, Fedict a besoin d'informations de contact valables.

Afin de toujours disposer d'une adresse e-mail valable, Fedict demande une adresse e-mail générique qui n'est pas liée à une personne, par exemple servicedesk@nomdel'organisation.be afin que chaque client puisse relayer l'information au sein de sa propre organisation.

Des coordonnées personnelles peuvent également être communiquées.

Vous trouverez ci-dessous un tableau dans lequel vous pourrez compléter les données.

Les champs grisés sont obligatoires. Les autres champs sont optionnels.

Coordonnées génériques *(pour communication générale relative aux services fournis par Fedict)*	Nom : Téléphone :	Adresse e-mail :
Gestionnaire de l'application	Nom : Téléphone :	Adresse e-mail :
Personne de contact technique	Nom : Téléphone :	Adresse e-mail :
Intégrateur (sous-traitant)	Nom : Téléphone :	Adresse e-mail :
Service Manager	Nom : Téléphone :	Adresse e-mail :
Autre :	Nom : Téléphone :	Adresse e-mail :