

Nom du service G-Cloud

Identification CSAM

Version 1.2 – 18/04/2018

Comprend les fonctionnalités :

- FAS – Federal Authentication Service
- SMA – Self Management Application / CSAM - Mes clés numériques

- Le FAS peut, à des fins d'autorisation par un service en ligne, utiliser le service « Attribute Publication Service » (APS) (de BOSA DG Transformation Digitale) pour rechercher dans des sources authentiques une série d'attributs (p.ex. des rôles) des utilisateurs finaux.
Attention : le service « Attribute Publication Service » ne fait cependant pas partie du FAS.

Description du service G-Cloud

L'« Identification CSAM » fait office de « voie d'accès centrale aux services en ligne de l'Administration » et organise le contrôle d'identité ainsi que la gestion de l'authentification au sein de l'e-gouvernement.

Utilisateurs (bénéficiaires) de l'« Identification CSAM » :

L'« Identification CSAM » s'adresse à l'ensemble des services et institutions publics qui souhaitent un processus d'authentification sécurisé pour leurs services (applications) en ligne :

- Services publics fédéraux et institutions publiques fédérales
- Communautés et Régions
- Provinces, communes et CPAS
- Instances chargées de la protection sociale ou de la sécurité sociale et acteurs des soins de santé
- Les entreprises ou personnes qui exécutent une mission pour le compte de l'Administration ; les institutions assumant des missions d'intérêt général, pour leurs missions d'intérêt général.

Les utilisateurs finaux de l'« Identification CSAM » :

Les utilisateurs finaux sont les « clients » des bénéficiaires qui ont accès, via l'« Identification CSAM », aux applications qu'ils souhaitent utiliser ; il s'agit de citoyens agissant en leur nom propre, de personnes agissant au nom d'une organisation ou d'une entreprise, ou encore de fonctionnaires ou de personnes mandatées.

Fonctionnement du service – Identification CSAM/FAS :

But : identification et authentification des utilisateurs pour accéder aux services en ligne de l'Administration.

Un utilisateur final qui se connecte à un service public en ligne (application) est dirigé vers le portail d'authentification CSAM (FAS).

Le FAS offre à l'utilisateur final un écran d'identification et lui demande ses identifiants.

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.

Attention : sur la base des identifiants, l'« Attribute Publication Service » peut demander des attributs de l'utilisateur final aux sources authentiques.

L'« Attribute Publication Service » ne recherche que les attributs provenant de sources authentiques (Registre national, registre BIS ou BCE) qui sont nécessaires à l'application pour octroyer une autorisation. Il ne recherche donc aucun autre attribut que l'application entend éventuellement utiliser elle-même.

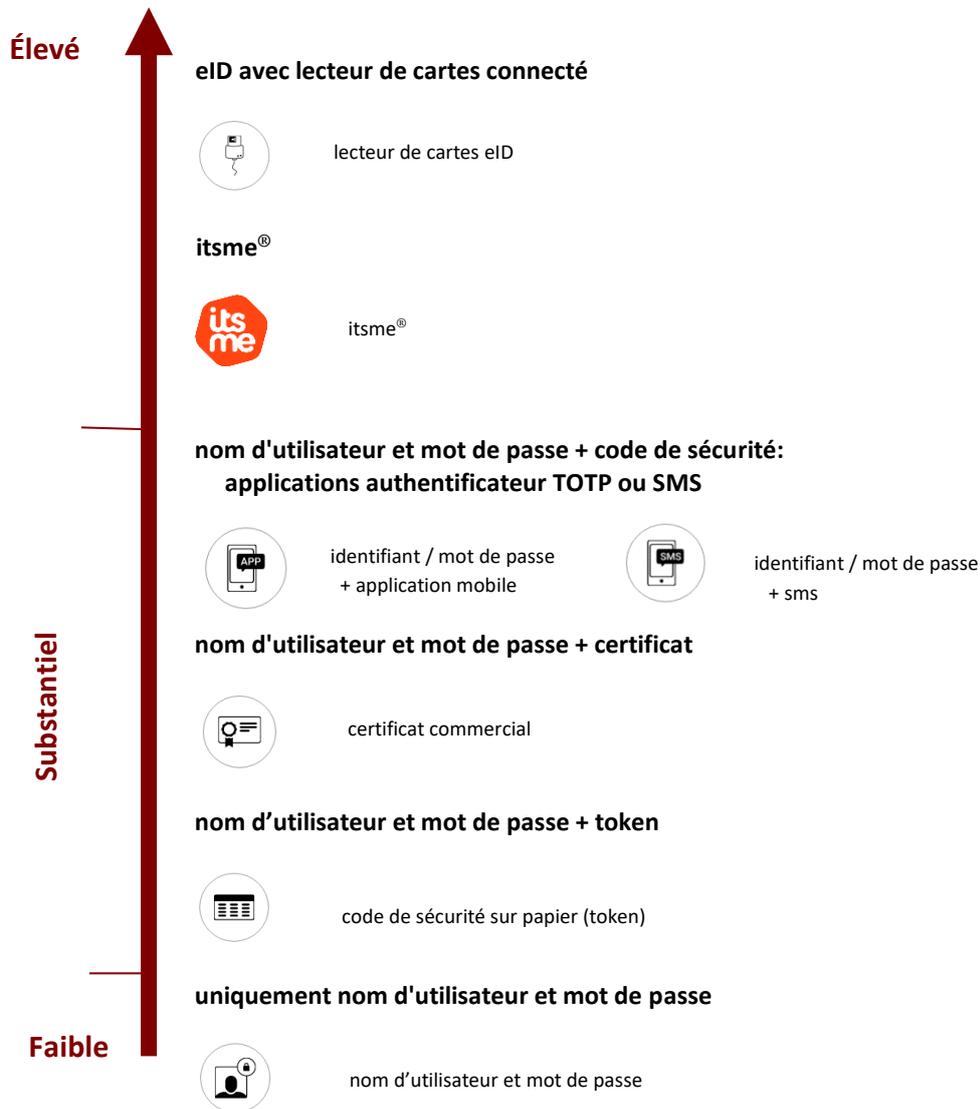
Sur la base du message de réponse, l'application réceptrice peut prendre la décision d'ouvrir une session pour l'utilisateur final.

C'est donc l'application (service public en ligne) elle-même qui, grâce au FAS, s'assure du fait que la personne est bien celle qu'elle prétend être, et qui décide si l'utilisateur final peut accéder à cette application (autorisation).

Si des attributs sont recherchés dans des sources authentiques par le biais du FAS (à des fins d'autorisation par l'application), la vie privée de l'utilisateur final est scrupuleusement respectée : les seules informations qui seront recherchées et disponibles sont celles pour lesquelles le service en ligne dispose d'une autorisation et dont il a effectivement besoin pour octroyer l'autorisation.

L'« Identification CSAM » propose plusieurs « clés numériques », qui sont réparties en différents niveaux de sécurité. La sensibilité des informations auxquelles l'utilisateur a accès dans les services en ligne ou dont il a besoin, détermine le niveau de sécurité. Le niveau de sécurité requis dépend donc du degré de confidentialité des informations utilisées par les services en ligne :

Ci-dessous les clés numériques actuelles, en ordre *décroissant* de niveau de sécurité.



Remarque :

[itsme®](#) est une initiative de [Belgian Mobile ID](#), et est « agréé » comme clé numérique au sein du FAS selon les modalités de l'[arrêté royal du 22 octobre 2017 qui fixe les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques.](#)

Une clé numérique assortie d'un niveau de sécurité plus *élevé* donne également accès à des services en ligne qui exigent une clé de niveau *inférieur*.

L'« Identification CSAM » n'offre actuellement aucune solution de gestion de l'identité et de l'accès aux utilisateurs *internes* (pour des applications *internes*) d'une organisation (p.ex. applications internes dans un AD au sein d'un service public).

Fonctionnement du service – SMA : Self Management Application

Cette fonctionnalité est offerte aux utilisateurs finaux dans « CSAM – Mes clés numériques ».

Ce module permet aux utilisateurs finaux de gérer eux-mêmes leurs coordonnées, ainsi que d'activer et de gérer leurs clés numériques.

Service owner

Le service « Identification CSAM » (tant le FAS que le SMA) et la gestion des services en la matière sont offerts par SPF BOSA DG Transformation Digitale.

Dans le cadre de l'utilisation de l'« Identification CSAM », des sources authentiques gérées par d'autres institutions publiques (Registre national, Registre BIS, BCSS et BCE) peuvent être consultées.

Service level agreements

- La disponibilité de l'« Identification CSAM » ne comprend pas les indisponibilités planifiées convenues pour la maintenance périodique et les activités de maintenance et mises en production convenues.

L'« Identification CSAM » vise la disponibilité (à savoir l'« objectif ») suivante :

Nom Service	Période	Objectif Disponibilité	Disponibilité réelle		
			2017	2016	2015
Identification CSAM	24 x 7	99,9%	99,93%	99,65%	99,78%

- Sur base annuelle, 4 versions majeures sont mises en production. Ces interventions se déroulent la nuit et nous nous efforçons d'obtenir une mise en production sans impact sur la disponibilité.
Il y a encore quelques mises en production mineures, mais qui n'ont pas non plus d'impact sur la disponibilité.
- En cas de calamités, une intervention 24h/24, 7j/7, est garantie.
- 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. (Note : le timing de « 1 semaine à l'avance » sera réexaminé).
- 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 signaler la restauration de la disponibilité.

- **Attention** : la disponibilité de l'« Identification CSAM » peut dépendre de la disponibilité de services sous-jacents :
 - sources authentiques
 - systèmes et infrastructure propres à BOSA DG Transformation Digitale
 - infrastructure de fournisseurs externes

Si l'« Attribute Publication Service » est activé pour la recherche d'attributs de l'utilisateur, la disponibilité de l'« Identification CSAM » peut être influencée si les sources authentiques ne sont pas disponibles.

La disponibilité maximale (objectif) de l'« Identification CSAM » est par conséquent égale à la disponibilité minimale des parties impliquées.

- Pour la performance de l'« Identification CSAM », les objectifs suivants en termes de délais de réponse ont été définis :

Identification CSAM	Norme	Objectif Temps de réponse	Réel 2017
User interface RT Transaction	< 2 sec	95 %	99,99 %
Application interface RT Transaction	< 0,1 sec	95 %	

- La prestation de services relative à l'« Identification CSAM » se fait sur la base du « meilleur effort » et aucune pénalité n'est prévue.
- Le Service Desk de BOSA DG Transformation Digitale est considéré, pour les services utilisés, comme l'unique point de contact pour les bénéficiaires de l'« Identification CSAM ».

Il est de la responsabilité du bénéficiaire d'offrir un support suffisant (de première ligne aux utilisateurs finaux) en termes d'équipements et de solidité pour ses propres services. En aucun cas, sauf disposition contraire, le Service Desk de BOSA DG Transformation Digitale ne fournira directement des services aux utilisateurs finaux du bénéficiaire.

- Le support aux services publics et institutions publiques (support de seconde ligne aux bénéficiaires) du lundi au vendredi de 8h30 à 17h30 (les jours d'ouverture de l'Administration fédérale) est offert par le Service Desk de BOSA DG Transformation Digitale.

Disponibilité	Contact	Lundi à vendredi
Service Desk de BOSA DG Transformation Digitale	Par téléphone Mail	8:30 - 17:00

- **Modèle de service de l'« Identification CSAM »**

L'« Identification CSAM » est un service mûr géré de bout en bout.

Les nouveaux bénéficiaires potentiels intéressés sont depuis les premiers contacts informés en détail sur les possibilités et conditions d'utilisation de l'« Identification CSAM ». Ces informations ne se limitent pas uniquement aux aspects techniques ou fonctionnels mais incluent aussi par exemple les obligations relatives à l'utilisation du numéro de Registre national.

Pour l'« onboarding » effectif, les bénéficiaires sont accompagnés par le Service Desk de BOSA DG Transformation Digitale ou peuvent même faire appel à une expertise externe via une centrale de marchés.

Une fois l'« Identification CSAM » implémentée, les bénéficiaires peuvent s'adresser au Service Desk de BOSA DG Transformation Digitale, qui sera le niveau d'escalade pour leurs propres services de support.

D'autres aspects sont pris en charge par l'« IAM Service Management » (p.ex. le reporting, l'activation d'autres méthodes d'authentification, ...).

- Obligations des bénéficiaires de l'« Identification CSAM »

Les conditions d'utilisation et les obligations des bénéficiaires de l'« Identification CSAM » sont fixées dans une convention d'utilisation contraignante et sont de nature diverse : technique, fonctionnelle, opérationnelle, juridique, audit, ...

- Veiller à une implémentation technique correcte de l'« Identification CSAM » selon les directives de BOSA DG Transformation Digitale
- Si le bénéficiaire fait appel à un intégrateur, veiller à ce que ce dernier respecte lui aussi strictement les obligations du bénéficiaire
- Veiller à ce que les fonctionnalités de l'« Identification CSAM » soient correctement mises en œuvre (p.ex. fonctionnalité de Single Logon / Single Logout)
- Disposer d'une autorisation du comité sectoriel du Registre national qui donne accès à des données du Registre national, ou disposer de l'autorisation générale (Délibération RN n° 21/2015 du 25 mars 2015) d'utiliser le numéro de Registre national en cas d'utilisation du FAS
- Lors du recours à l'« Identification CSAM », respecter la législation sur la protection de la vie privée
- Prévoir une piste d'audit pour toutes les transactions passant par l'« Identification CSAM »
- (Énumération non limitative)...

- Évolutivité de l'« Identification CSAM »

- En termes de capacité, l'« Identification CSAM » permet une évolutivité linéaire, avec maintien de la performance, de la disponibilité et de la fiabilité actuelles (voir seuils ci-dessus).
- Le recours à l'« Identification CSAM » pendant la période Tax-on-Web (= charge en période de pointe) représente environ 30% de la capacité totale disponible.
- À partir de 2018, l'« Identification CSAM » sera aussi mise à disposition sur des plateformes virtuelles en tant que « modèle hébergé » (« hosted model »).
- Depuis 2017, des versions majeures et mineures du « FAS / Identification CSAM » sont mises en production sans impact sur la disponibilité, la performance et la fiabilité, mais avec une réduction temporaire restreinte de la capacité totale.

L'utilisation de l'« Identification CSAM » (tant pour les méthodes d'authentification/clés numériques agréés que pour les propres méthodes/clés) est gratuite pour les utilisateurs finaux et les bénéficiaires.

(Exception : clé numérique SMSOTP ; les frais d'envoi du SMS sont à la charge du bénéficiaire.)

Le paiement éventuel dû aux responsables des sources d'informations pour les services de la source d'information (= sources authentiques) est à charge des bénéficiaires de l'« Identification CSAM » qui recourent aux services de cette source d'information.

Quelle est l'évolution prévue pour ce service ?

Missions principales futures de l'« Identification CSAM » :

- Faire office de « hub » pour l'authentification externe, notamment en liant de nouvelles méthodes d'authentification de services externes « agréés » à l'« Identification CSAM » en tant que service d'authentification de confiance
- Anonymisation des utilisateurs (attributs) à l'égard des applications
- Gestion « Single Sign On »
- Traduction en numéro de Registre national
- Conformité au Règlement eIDAS ; identification électronique et services de confiance
- Conformité au GDPR

Fonctionnalités importantes mises en production

- « Identification CSAM » - Levels of Assurance, de la clé numérique au niveau de sécurité (rel. 12.0.0 – Jan 2017)
- TMA – application pour tester le login eID après l'installation du middleware eID (rel. 13.0.0 – Avr 2017)
- Profil aisément accessible (authentification faible) avec « step-up » possible (rel. 14.0.0 – Déc 2017)
- Life cycle management sur des clés numériques et des coordonnées des utilisateurs finaux (rel. 15.0.0 – Fév 2018)
- Forte authentification mobile via des partenaires agréés (Jan 2018 – itsme® en production dans le FAS)
- « Identification CSAM » pour non-titulaires de l'eID (modèle LRA) (Avr 2018 – des séances d'information à l'intention des villes et municipalités en cours)

Fonctionnalités éventuelles importantes prévues dans le futur :

- Profil de base /signalétique du citoyen
- Utilisation généralisée de l'« Identification CSAM » pour la Sécurité sociale
- « Identification CSAM » - life cycle management des personnes et entreprises
- « Identification CSAM » pour non-titulaires de l'eID (modèle LRA)
- Identification et enregistrement à distance pour les non-titulaires de l'eID
- « Identification CSAM » sur plateformes virtuelles en tant que « modèle hébergé » (« hosted model »).

Objectifs 2018-2020:

- 100% des authentifications pour les utilisateurs de services en ligne de l'Administration ont lieu via l'« Identification CSAM »
- 100% des services en ligne de l'Administration utilisent l'« Identification CSAM » pour l'authentification de leurs utilisateurs
- Les services en ligne de l'Administration proposent toutes les méthodes d'authentification (« clés numériques ») qui mettent à disposition l'« Identification CSAM », pour l'accès de leurs utilisateurs

Aspects pratiques

Infos et demandes à : csam@gcloud.belgium.be