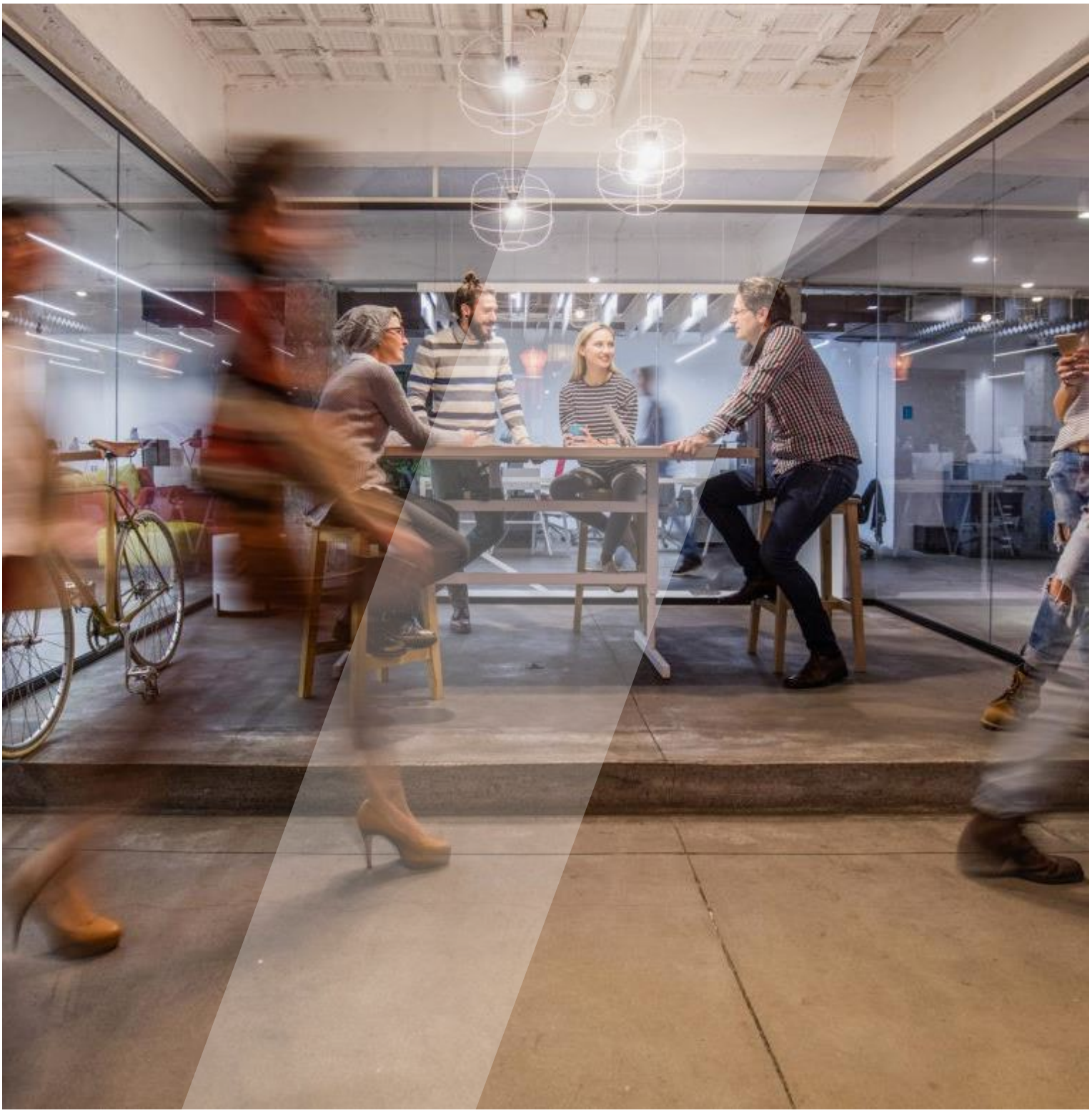


Signals

Livre blanc de la sécurité

Table des matières

Contrôle des versions

Date	*Version*	*Description des changements*	*Responsable*
23-11-2021	1.0	Version initiale	Vincent Roodenburg
18-03-2022	2.0	- liens hypertexte corrigés - ajout de la section "Sécurité dans le processus de développement".	Vincent Roodenburg
31-05-2022	3.0	Mise à jour du lien vers la déclaration de confidentialité	Vincent Roodenburg
13-02-2023	4.0	Lien inclus vers le livre blanc d'OKTA sur la sécurité	Cor van de Merwe
28-05-2024	4.01	Rebranding Mazars to Forvis Mazars	Jan-Benedikt Weber

Présentation de la plateforme Signals de Mazars

Généralités

Signals est la plateforme de collaboration numérique de Forvis Mazars. Signals est une plateforme basée dans le cloud, entièrement adaptative et qui peut être utilisée sur un ordinateur, une tablette et un smartphone. La plateforme est utilisée par les clients et les employés de Forvis Mazars pour travailler ensemble en ligne. Les principales fonctionnalités sont :

- demander des informations à nos clients via des " demandes d'approvisionnement ".

- d'approuver des tâches via des workflows

- de soumettre les déclarations fiscales aux autorités locales

Signals fait partie d'un écosystème basé dans le cloud et fonctionne comme une "porte d'entrée" permettant à tous nos clients d'interagir avec Forvis Mazars. Par cette porte, les clients peuvent se connecter à d'autres applications (cloud).

Demande d'approvisionnement

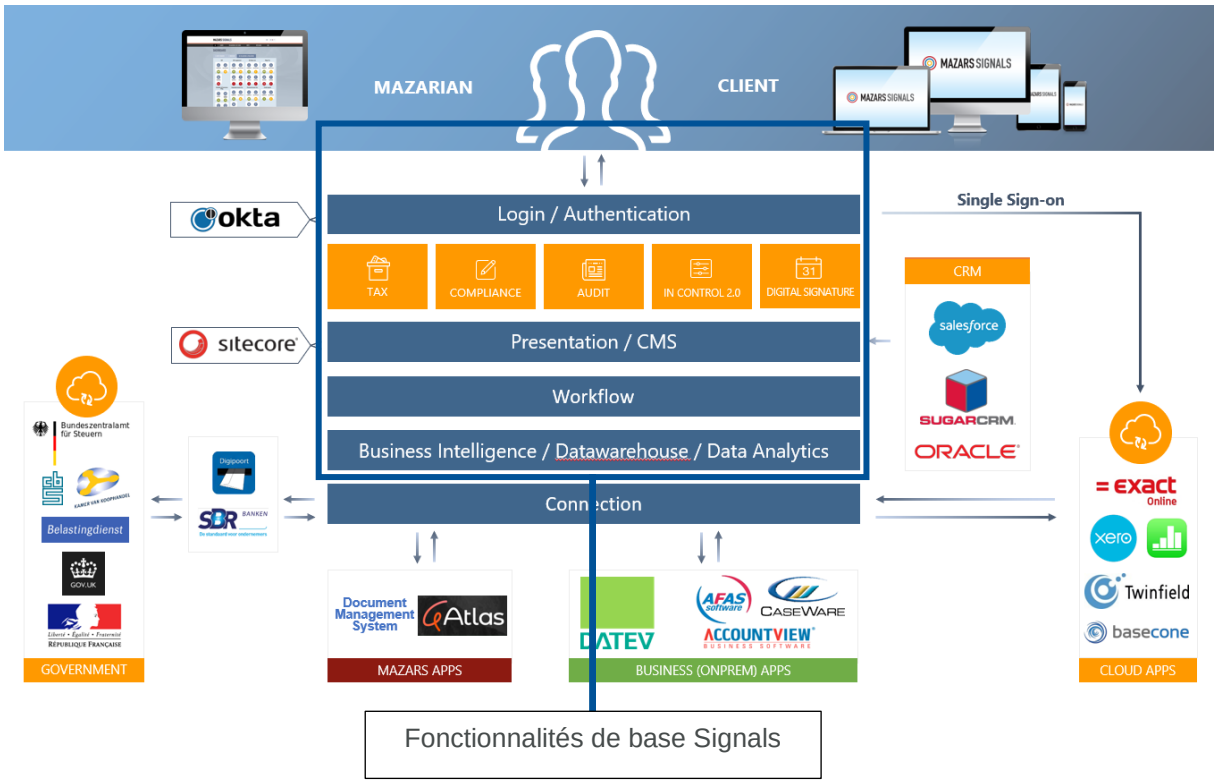
Forvis Mazars préparera une demande d’approvisionnement dans Signals afin de collecter les informations et les documents nécessaires à la fourniture du service. Les clients doivent se connecter à Signals et envoyer les documents demandés. Lorsque toutes les informations sont fournies, les clients marquent la demande d’approvisionnement comme complète et l'envoient à Forvis Mazars. Une fois que Forvis Mazars a approuvé les demandes d’approvisionnement, tous les documents sont enregistrés dans leur(s) application(s) de back-office. Toutes les actions relatives aux demandes d’approvisionnement sont enregistrées dans une piste d'audit.

Workflows et déclarations fiscales

Forvis Mazars présente les travaux préparés (rapports annuels, déclarations fiscales) à ses clients en utilisant Signals. Les rapports et les déclarations fiscales sont préparés dans les systèmes de back-office et ensuite téléchargés sur Signals. Les clients peuvent soumettre des tâches et leurs déclarations seront directement envoyées aux autorités fiscales via un processus automatisé. Toutes les actions concernant les déclarations effectuées par les clients et les employés sont stockées dans une piste d'audit complète.

Plateforme

Ce schéma représente l'état de l'écosystème de Signals:



Chiffrement

Les données au repos et les données en transit sont chiffrées à l'aide des normes industrielles de chiffrement. Toutes les mesures de chiffrement sont mises en œuvre pour garantir la confidentialité et l'intégrité des données au sein de Signals.

Gestion des données et conformité

Tous les systèmes liés à Signals sont situés aux Pays-Bas et en Irlande (Microsoft Azure West-Europe). Le traitement des données a lieu conformément aux lois et réglementations de l'UE. Pour se conformer aux exigences du RGPD, aucune donnée à caractère personnel (DCP) n'est transférée en dehors des frontières de l'UE. La conservation des données des clients respecte les délais légaux (avec un maximum de 10 ans).

Depuis novembre 2020, Microsoft applique des mesures de protection de la vie privée supplémentaires appelées "Defending your data", pour protéger les données des clients, comme décrit dans cet article : **New steps to defend your data - Microsoft On the Issues**

Pour connaître les mesures de protection supplémentaires de Microsoft par rapport aux clauses contractuelles standard, lisez le document suivant : **REFERENCE-COPY-Additional-Safeguards-Addendum-to-Standard-Contractual-Clauses-.pdf (microsoft.com).**

(Addendum aux clauses contractuelles standard de Microsoft).

Disponibilité et fiabilité

Nous surveillons en permanence les performances de nos services et disposons de notifications automatiques pour garantir une réponse rapide en cas d'éventuelles interruptions de service. Toutes les modifications de code sont vérifiées et approuvées avant d'être déployées sur les serveurs de production. Nous suivons de près les mises à jour de sécurité et mettons immédiatement à jour nos systèmes lorsque de nouvelles vulnérabilités sont découvertes.

Infrastructure

Hébergement

Tous les systèmes de serveurs sont hébergés dans Microsoft Azure, en Europe occidentale, avec Amsterdam comme site principal et Dublin comme site secondaire. Les centres de données de Microsoft sont conformes à plusieurs certifications. Veuillez consulter **https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/** pour tous les détails.

Processus d'application des correctifs

Tous les systèmes serveurs font l'objet de correctifs réguliers (au moins une fois par mois) afin de maintenir le plus haut niveau de sécurité.

Surveillance

Tous les systèmes concernés sont surveillés 24 heures sur 24, 7 jours sur 7, afin de garantir la disponibilité la plus élevée. Les ingénieurs reçoivent des alertes automatisées lorsqu'il y a une interruption possible d'un système de production.

Mesures de sécurité

Veuillez consulter **https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security** pour connaître toutes les mesures de sécurité (physique) mises en place dans les centres de données Microsoft Azure.

Application

Identification, authentification et autorisation

Seuls les comptes utilisateurs vérifiés et d'employés Forvis Mazars ont accès à certaines données des clients au sein de la plateforme Signals .

Les clients s'authentifient via la plateforme Okta, où l'authentification multi-facteurs (MFA) est obligatoire et appliquée depuis l'application Okta Verify, disponible pour Android et iOS. Veuillez consulter **https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/** pour plus d'informations sur les mesures de sécurité applicables à la plateforme Okta.

Les employés de Forvis Mazars qui se connectent depuis le réseau Forvis Mazars, bénéficient du SSO pour accéder à Signals. En fonction de leur rôle, les employés de Forvis Mazars n'ont accès qu'à certaines données clients. Les rôles d'administrateurs fonctionnels et techniques sont limités à Forvis Mazars. Ce type de privilège n'est autorisé qu'après validation des antécédents du personnel.

Administration

L'accès à l'administration du système et au développement des applications est limité à un nombre restreint d'administrateurs système et de développeurs d'applications. Les accords appropriés concernant la non-divulgation et la confidentialité sont signés par chaque administrateur système et développeur.

L'accès à l'administration fonctionnelle est limité à un nombre restreint d'administrateurs fonctionnels et de gestionnaires de la relation client. Les accords appropriés de non-divulgation et de confidentialité sont signés par chaque administrateur fonctionnel.

Processus de développement

Le processus de développement se fait de manière agile. Forvis Mazars fournit le propriétaire du produit, qui est une fonction clé dans un processus de développement agile.

La sécurité dans le processus de développement

Nous réalisons des revues de code et utilisons l'analyse statique du code pour identifier les risques de sécurité. Les risques identifiés sont ensuite évalués et réduits si nécessaire. Nous appliquons les pratiques du cycle de vie de la sécurité du développement de Microsoft:

Gérer le risque de sécurité lié à l'utilisation de composants tiers:
Nous inventorié les composants tiers que nous utilisons et nous sommes en train d'automatiser cet inventaire.

Nous évaluons aussi régulièrement les dépendances à ces composants, par exemple en ce qui concerne la fin de vie d'un tel composant.

Réalisation de tests de sécurité par analyse statique (SAST)
Nous utilisons SonarCloud pour identifier et analyser les points sensibles en matière de sécurité.

Réalisation de tests d'intrusion
Nous effectuons des tests de sécurité avant la mise en production de chaque nouvelle application et nous effectuons un test d'intrusion au moins une fois par an.

Déploiement

Forvis Mazars travaille avec un calendrier de déploiement mensuel. Un déploiement est prévu chaque mois, généralement entre le 14 et le 20 du mois. Le scrum master décide avec les product owners quels travaux ont été marqués comme réalisés dans les sprints 1-2 avant d'être déployés de façon incrémentale dans l'environnement de production. La procédure de déploiement est la suivante :

1. Sélectionner les histoires finalisées qui doivent être diffusées dans l'environnement de production.
2. Fusionner les stories de notre branche de développement avec la branche principale.
3. Déployer les stories dans l'environnement de test principal
4. Toutes les stories sont testées sur l'environnement de test principal et des tests de non-régression sont réalisés dans l'environnement entier.
5. Déploiement de toutes les stories dans l'environnement d'acceptation
6. Des tests de non-régression sont réalisés dans tout l''environnement d'acceptation.
7. Déploiement de toutes les stories dans l'environnement de production
8. Après le déploiement, des contrôles de l'état de santé sont effectués pour vérifier le déploiement. Dans les jours qui suivent le déploiement, l'équipe de développement vérifie activement la surveillance et les fichiers de log.

Après la revue du sprint, le product owner décide s'il veut déployer le nouvel incrément dans l'environnement de production.

Feuille de route du produit et estimations à long terme

La feuille de route produit donne la vision à plus long terme. Le product owner, avec ses partenaires, est le principal moteur de la feuille de route produit. Les développeurs jouent également un rôle en aidant Forvis Mazars à créer cette feuille de route à un niveau stratégique. La feuille de route produit doit montrer la direction que prend le produit et la valeur qu'il apportera à Forvis Mazars et à ses clients.

Une feuille de route produit est constituée d'épopées. Il s'agit d'éléments de haut niveau qui sont trop volumineux pour être traités indépendamment et qui seront décomposés en plusieurs sous-éléments, par exemple : la signature numérique des rapports de fin d'année.

Pour la feuille de route, l'équipe peut faire des estimations de haut niveau avec le product owner. Ces estimations sont généralement faites rapidement, car l'objectif n'est pas d'essayer de répondre à toutes les exigences du départ. Les estimations de haut niveau servent plutôt à indiquer l'ampleur prévue du développement d'une épopée.

Une fois le développement commencé, ces estimations fluctuent au fur et à mesure que les stories sont affinées et que les résultats requis pour stories deviennent plus clairs. Il est toujours bon de garder ces fluctuations à l'esprit lors de la planification.

Mesures de sécurité supplémentaires

En outre, Signals est protégé par des contrôles de sécurité au niveau de la couche application.

Tests de sécurité

La plateforme Signals de Forvis Mazars est régulièrement testée par un tiers indépendant afin de garantir l'objectivité des résultats. La correction des vulnérabilités éventuelles est toujours effectuée dans l'ordre de leur criticité.

Protection de l'intégrité des journaux d'audit

Les fichiers journaux de Signals et les pistes d'audit sont stockés sur des disques virtuels, où le chiffrement au repos est appliqué. L'accès aux fichiers journaux et aux pistes d'audit est limité à un nombre restreint d'administrateurs système.

Organisation

Vie privée

Nous prenons très au sérieux la sécurité et la confidentialité des données de nos clients et les traitons comme un indicateur important. Signals est conforme au RGPD. Pour les pays hors de l'UE, veuillez consulter les réglementations locales en matière de confidentialité et, le cas échéant, consulter les clauses contractuelles types supplémentaires pour les transferts de données entre les pays de l'UE et les pays hors de l'UE. Vous pouvez consulter un aperçu complet de notre politique de confidentialité sur **https://www.mazarssignals.nl/en/privacy-statement**.

Politiques de sécurité

Tous les employés appliquent des politiques de sécurité formalisées couvrant l'utilisation, le traitement des données confidentielles, etc.

Reprise après sinistre / sauvegardes

Les données des applications et des clients sont hébergées de manière redondante dans plusieurs zones de stockage, avec des sauvegardes disponibles pour la récupération en cas de sinistre.

Gestion des incidents de sécurité

Dans le cas d'un incident de sécurité avéré pour lequel des données clients seraient compromises, notre équipe vous en informera rapidement. Si votre équipe sécurité a besoin de journaux d'événements supplémentaires pour ses investigations sur un incident concernant votre organisation, notre RSSI se chargera de fournir le nécessaire.

Point de contact unique pour la sécurité

Afin de répondre aux questions concernant ce document, veuillez envoyer vos demandes à **security@mazars.nl**.