Signals

Security whitepaper

Classification: public

mazars

Table of contents

mazars

Version control

Date	*Version*	*Description of changes*	*Responsible*
23 November 2021	1.0	Initial version	V. Roodenburg
18 March 2022	2.0	- corrected hyperlinks - added section “Security in the development process”	V. Roodenburg
31 May 2022	3.0	Updated link to privacy statement	V. Roodenburg
13 February 2023	4.0	Included link to OKTA security whitepaper	C. van de Merwe

mazars

Introduction to Mazars' Signals platform

Generic

Signals is the digital collaboration platform for Mazars. Mazars Signals is a cloud-based platform, fully responsive and can be used on desktop, tablet and mobile devices. The platform is used by clients and Mazars employees to work together online. The main features are:

- request information from our clients through 'supply requests'
- to approve task through workflows
- to submit tax returns to local authorities

Mazars' Signals is part of a cloud-based ecosystem and functions as a 'front door' for all our clients to interact with Mazars. Through this door clients can login to other (cloud) applications.

Supply Request

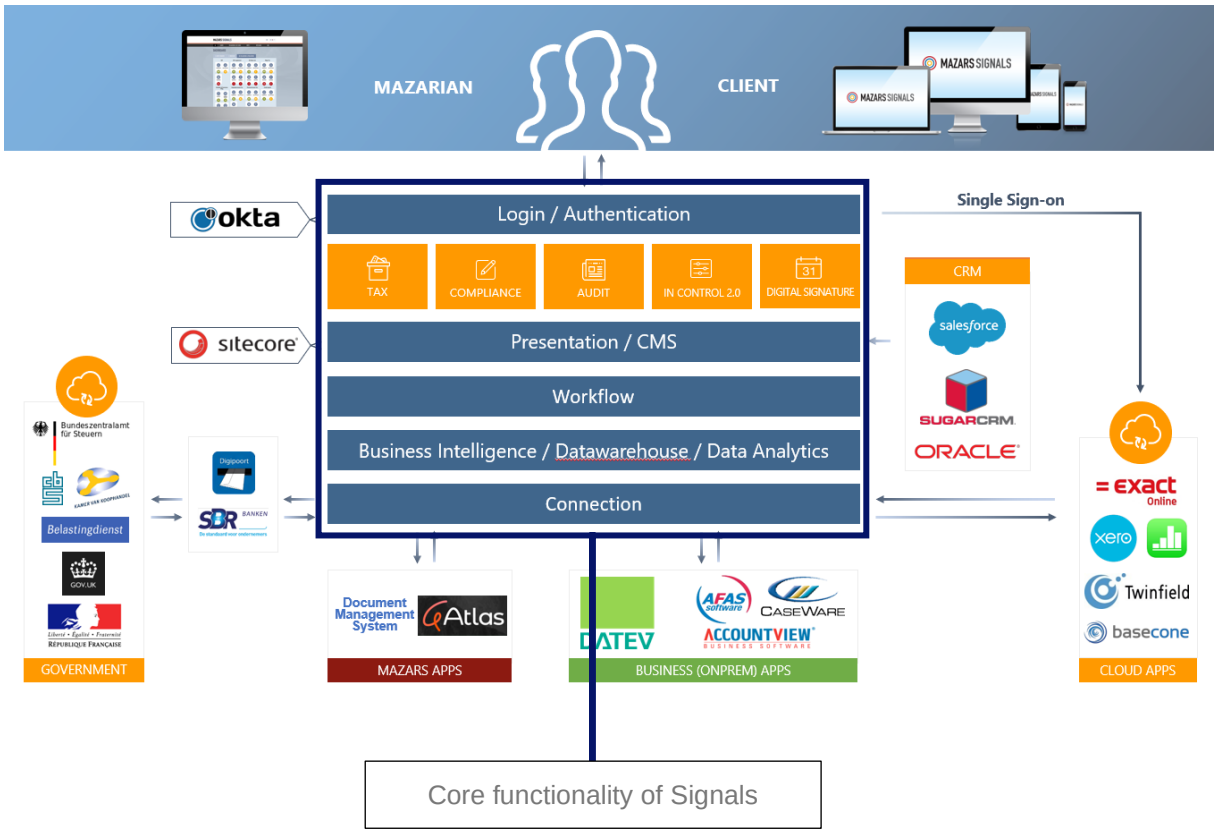
Mazars will prepare a supply request in Signals in order to request the necessary information and documents to provide their services. Clients have to log in to Signals and will upload the requested documents. When all information is provided, clients mark the supply request as complete and sent it to Mazars. After Mazars approves the supply requests all documents will be saved in their back-office application(s). All actions involving the supply requests are stored in an audit trail.

Workflows & tax returns

Mazars presents the prepared work (annual reports, tax returns) to our clients using Signals. The reports and tax returns are prepared in back-office systems and then uploaded onto Signals. The clients can submit task and their declarations which will directly be sent to the Tax Authorities through an automated process. All actions involving the declarations performed by both clients and employees are stored in a full audit trail.

Platform

This figure represents the status of the Signals ecosystem:



Encryption

Both data-at-rest and data-in-transit are encrypted using industry standards of encryption. All encryption measures are implemented to ensure the confidentiality and integrity of the data within Signals.

Data Management and Compliance

All related Mazars Signals systems are situated in The Netherlands and Ireland (Microsoft Azure West-Europe). Data processing takes place according to EU laws and regulations. To comply with GDPR requirements, no Personally Identifiable Information (PII) is transferred outside EU borders. Customer data is retained according to comply with legal retention periods (with a maximum of 10 years).

Since November 2020, Microsoft has applied additional privacy protections called “Defending your data”, to protect customer data as described in this article: New Steps to Defend Your Data - Microsoft On the Issues.

To learn about Microsoft’s Additional Safeguards to Standard Contractual Clauses, it is relevant to take notice of the following document: REFERENCE-COPY-Additional-Safeguards-Addendum-to-Standard-Contractual-Clauses-.pdf (microsoft.com).

(Microsoft’s Additional Safeguards Addendum to Standard Contractual Clauses).

Uptime & Reliability

We constantly monitor our service performance and have automatic notifications to ensure rapid response for possible service interruptions. All code changes are verified and approved before deploying to production servers. We closely monitor updates from the security community and immediately update our systems when new vulnerabilities are discovered.

Infrastructure

Hosting

All server systems are hosted within Microsoft Azure, within the West-Europe region, with Amsterdam as the primary location and Dublin as the secondary location. Microsoft data centres comply with several certifications. Please check https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/ for all details.

Patching Process

All related server systems are patched regularly (at least monthly) to maintain the highest security standards possible.

Monitoring

All related server systems are monitored 24/7 to ensure the highest possible uptime. Engineers receive automated alerts when there is a possible interruption of any production system.

Security Measures

Please check https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security for all (physical) security measures applicable within the Microsoft Azure data centre facilities.

Application

Identification, authentication & authorisation

Only verified user and (Mazars) employee accounts have access to specific customer data within Mazars' Signals platform.

Client users authenticate applying the Okta platform, where Multi-Factor Authentication (MFA) is mandatory and is applied through the Okta Verify app, available for Android and iOS. Please check https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/ for more information on the security measures applicable to the Okta platform.

Mazars employees who login within the confinements of the Mazars network, use SSO to access Signals. Depending on their role, Mazars employees only have access to specific customer data. Functional and technical administrator roles are limited within Mazars' organisation. These kind of privileges are only allowed when extra background checks are compliant and verified.

Administration

Access to system administration and application development purposes, is restricted to a limited number of system administrators and application developers. The appropriate agreements regarding non-disclosure and confidentiality are signed by each system administrator and developer assigned to perform system administration tasks and development tasks.

Access to functional administration purposes is restricted to a limited number of functional admins and customer/relationship managers. The appropriate agreements regarding non-disclosure and confidentiality are signed by each functional administrator assigned to perform functional administration tasks.

Development process

The development process is done in an agile way. Mazars delivers the product owner, which is a key function in an agile development process.

Security in the development process

We perform code reviews and use static code analysis to identify security risks. Identified risks are then evaluated and resolved where necessary. We perform the following practices from Microsoft's Security Development Lifecycle:

Manage the Security Risk of Using Third-Party Components:
We have created overviews of which Third-Party components we use and we are in the process of automating this inventory.

We also regularly evaluate such dependencies, for example regarding an approaching End-of-Life date on such a component.

Perform Static Analysis Security Testing (SAST)
We use SonarCloud for identification and analysis of security hotspots.

Perform Penetration Testing
We run security tests before every new application release to production and we run a penetration test at least once a year.

Rollout

Mazars works with a monthly deployment schedule. There is a deployment scheduled every month, typically between the 14th and the 20th of the month. The scrum master will decide together with the product owners what work that has been marked as done in the 1-2 sprints before will be released as an increment to the production environment. The rollout procedure is as follows:

1. Select the finalised stories that need to be released to the production environment
2. Merge the stories from our development branch to the main branch
3. Deploy the stories to the main test environment
4. All stories are tested on the main test environment and the entire environment is regression tested
5. Deploy all stories to the acceptance environment
6. The acceptance environment is fully regression tested
7. Deploy all stories to the production environment
8. After deployment sanity checks are done to verify the deployment. During the days after the deployment the development team will actively check monitoring and log files.

After the sprint review the product owner decides if he wants to roll out the new increment to the production environment.

Product roadmap & long-term estimations

For longer-term vision a product roadmap is in place. The product owner, together with his stakeholders, is the key driver behind the product roadmap. Developers also play a role in assisting Mazars with creating this roadmap on a strategical level. The product roadmap should show the direction the product is growing and the value this will bring to Mazars and its clients.

A product roadmap consists of epics. These are high-level chunks of work that are too big to be worked on independently and will be broken down into multiple stores, e.g.: digital signing of year-end reports.

For the roadmap the team can make high-level estimations together with the product owner. These estimations are usually done rapidly as the goal is not to try to solve all the requirements up-front. Instead high-level estimations are given to indicate the expected scope of developing an epic.

Once development starts these estimations will fluctuate as the stories are refined and the required outcomes for the stories become clearer. It is always good to keep these fluctuations in mind when planning.

Additional security measures

Additionally, Signals is protected by application layer security controls.

Security testing

Mazars' Signals platform is tested regularly for security vulnerabilities by an independent party to guarantee objectivity. Mitigation of possible vulnerabilities is always performed in order of their related criticality.

Protection of audit log integrity

Signals logfiles and audit trails are stored within virtual disks, where encryption-at-rest is applied. Access to logfiles and audit trails is restricted to a limited number of system administrators.

Organisation

Privacy

We take the security and privacy of our customer data very seriously and treat it as an important metric. Mazars' Signals complies to GDPR/EU regulations. For countries outside the EU, please consult local privacy regulations and, where applicable, consult additional standard contractual clauses for data transfers between EU and non-EU countries. You can consult a complete outline of our privacy policy at https://www.mazarssignals.com/en/privacy-statement.

Security policies

All employees are governed by documented security policies covering acceptable use, confidential data handling, etc.

Disaster recovery / backups

Application and customer data is stored redundantly at multiple availability zones with backups available to recover in the event of a disaster.

Security Incident Management

In the event of a confirmed security breach where customer data is compromised, our team will promptly notify you. Should your security team need additional logs for their investigation of an incident determined to affect your organisation, our Security Officer will coordinate responsibly to provide this as needed.

Single point-of-contact for security

In order to address questions regarding this document, please send your questions to security@mazars.nl.