Symbio

CLOUD OPERATION

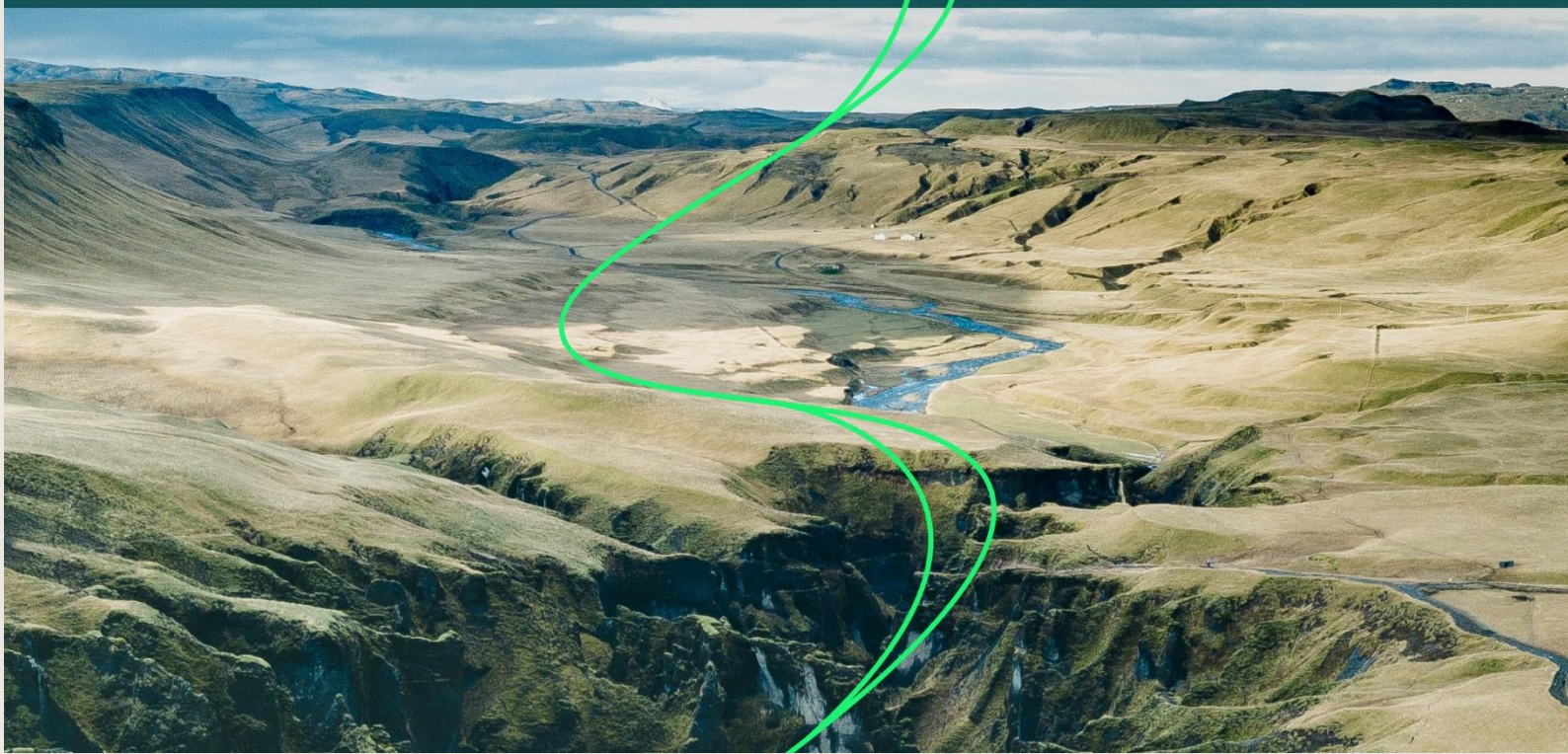


Table of content

1 Symbio Cloud Operation

Based on the previous chapter, the cloud-specific settings and properties are described. Cloud provider information, encryption and data protection information is explained.

1.1 General information about the cloud provider

Unless otherwise agreed, Symbioworld GmbH uses the Symbio Cloud Platform Services (PaaS) and Infrastructure Services (IaaS) from Microsoft Azure for the Symbio Cloud product.

For further general information about Microsoft Azure please see:
https://azure.microsoft.com/en-gb/

1.2 Where is your data?

Unless you have made other contractual agreements, your data will be stored in Microsoft's **European** data centers. All platform and infrastructure services store your data exclusively on European servers.

If desired, you can also apply for a private cloud in Germany with German data trust. Please contact us directly if you are interested in this service. All further information on data protection relates to the European cloud.

Further information provided by Microsoft:
https://www.microsoft.com/en-gb/trustcenter/privacy/where-your-data-is-located

For customers operating in highly regulated industries or countries with data protection laws, it is particularly important to know the geographic location of the data you have entrusted to a Microsoft Cloud Service. Microsoft also understands that some customers need to keep their data in a specific geographic location, e. g. within the European Union (EU). That's why Microsoft has a growing network of data centers around the world, ensuring that each data center meets the stringent security requirements of each and every data center.

- Customer data can be replicated within a geographic area to improve data life span in the event of a major data center emergency. In some cases, they are not replicated outside this area.
- Microsoft complies with data protection laws regarding the transfer of customer data across national borders. Example:
    - In order for international companies to benefit from the continuous flow of information required (including cross-border transfer of personal data), many Microsoft Cloud Services for Business customers offer EU standard contractual clauses with additional contractual safeguards for the transfer of personal data within the scope of the service. The Implementation of EU standard contractual clauses has been reviewed by EU data protection authorities and is in line with the strict data protection standards governing the international transfer of data by companies operating in EU member states.
    - In addition to our obligations under the standard contractual clauses and other model contracts, Microsoft is certified by the EU-U. S. Privacy Shield Framework, as set out by the U. S. Department of Commerce with regard to the collection, use and retention of personal data transferred from the EU to the United States. Microsoft's participation in

the Privacy Shield applies to all personal data that is subject to the Microsoft Privacy Statement and originates from the EU, the European Economic Area and Switzerland. Microsoft also complies with Swiss data protection laws regarding the processing of personal data from the European Economic Area and Switzerland.

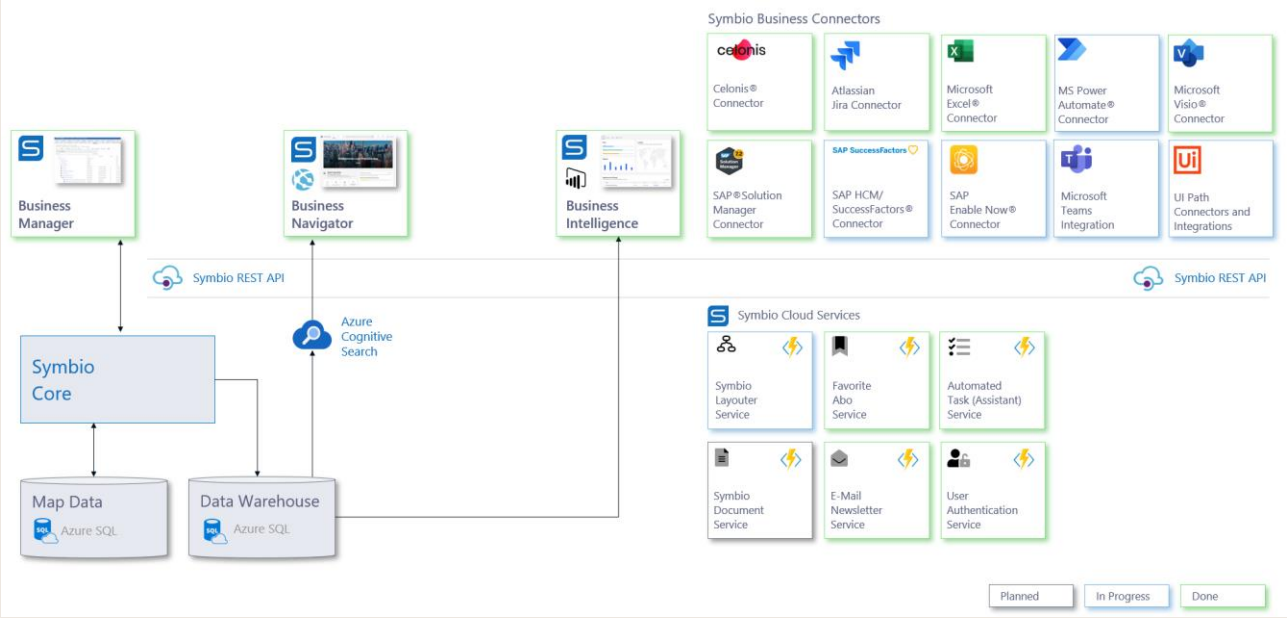
- Microsoft does not transfer any data to third parties (including for storage purposes) that you provide to Microsoft in connection with your use of our cloud services to companies covered by the Microsoft Online Services Terms of Service.

Microsoft does not control or restrict the locations from which customers or their end users access their data, regardless of where the customer data is stored.

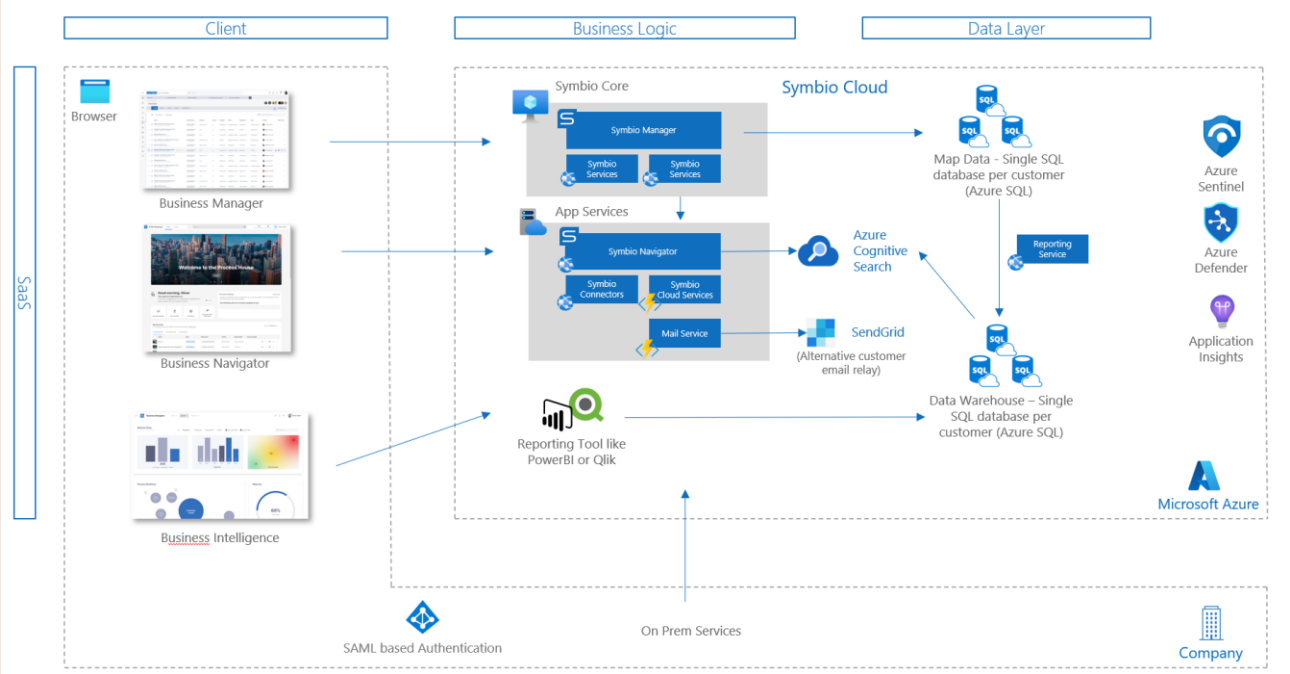
2 Cloud Overview

Symbio Cloud Architecture Overview

2.1 Symbio Apps, Services and Connectors

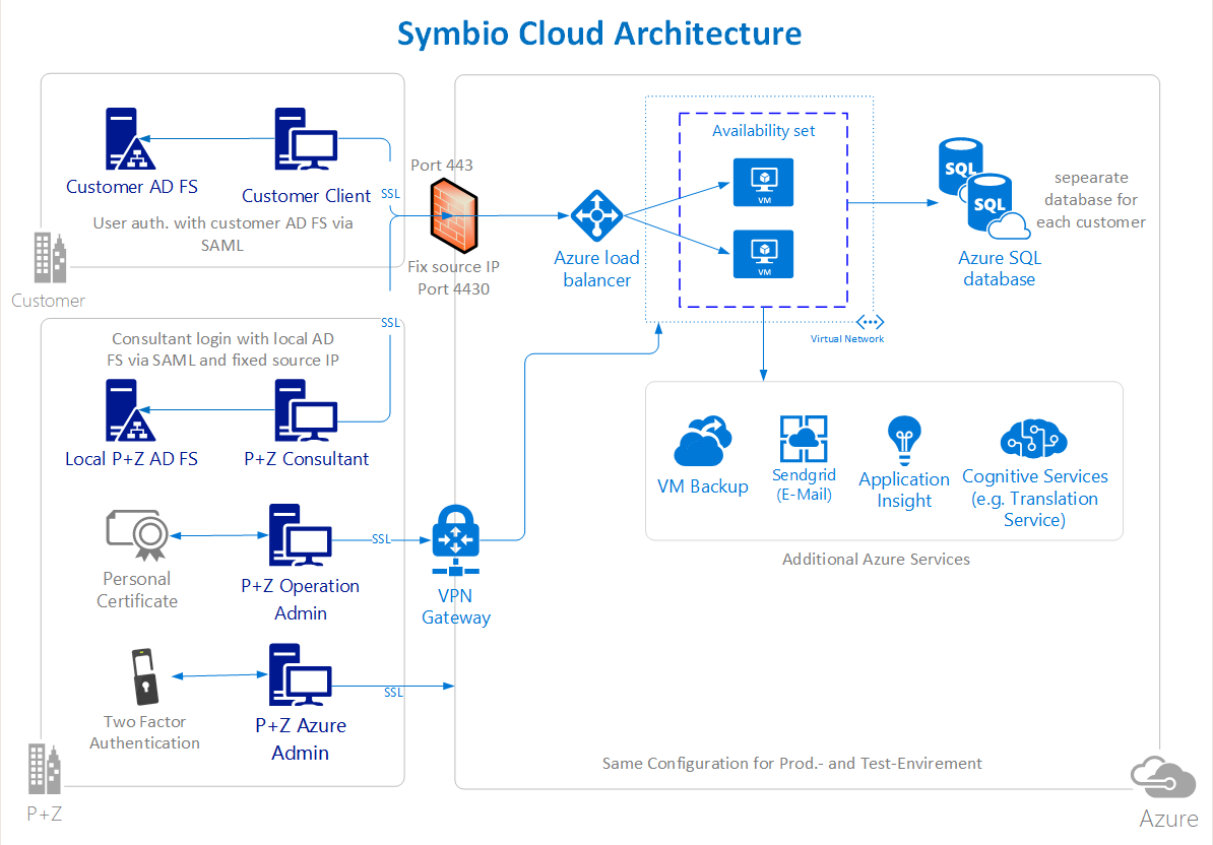


2.2 Symbio Azure Cloud Overview



2.3 Symbio Cloud Architecture Detailed

The following architectural image shows the basic structure of the Symbio Cloud.



3 Symbio Cloud Variants

3.1 Symbio Cloud Variants Overview

As a customer you can choose between the following cloud alternatives.

3.1.1 Standard / Professional Cloud

- No Symbio customizing possible, i.e.
  - Symbio Standard BPMN Method is used
  - Manuals/Theme settings can be individually adjusted, however
- Automatic updates / upgrades
- A single Azure SQL database for each customer

3.1.2 Enterprise Cloud

- Symbio customizing possible
- Updates / upgrades can be timed
- A single Azure SQL database for each customer
- A single Symbio instance for each customer

3.2 Symbio instance settings

Symbio instance settings can be customized in the Exclusive Cloud. The default values are described below, which also apply to the standard cloud.

3.2.1 Rendering update interval

Diagrams are checked every 30 seconds for updates in the background.

3.2.2 Free & Easy DB

Databases starting with "Sandbox" become sandboxes, i.e. the release workflow is not activated in these sandboxes.

3.3 Logging and tracing

3.3.1 Symbio

Each Symbio instance has only one single log file, i.e. in the standard cloud, a customer can see the log messages of another customer and possibly also the URLs if errors have been recorded. These log files can only be viewed by users with the application role "Administrator".

- These log files can be viewed online for 30 days.
- By default, only errors are logged.
- For analysis purposes, e. g. SAML connection for Active Directory, the logging level can be increased for a short time. Sensitive data is also recorded here, e. g. claims from Active Directory, but never passwords.

3.3.2 IIS

By default, the IIS web server records the individual requests (IP, URL, user, etc.). The IIS logs are only visible to the operations team and can be evaluated for performance analyses.

3.3.3 Windows

Windows records typical log messages for Symbio as an application that can only be viewed by the operations team.

3.3.4 Databases

In Azure SQL, log messages are recorded for each database and remain visible only to the operations team.

3.3.5 Performance

With the help of Azure Application Insights, in addition to typical web statistics (browser version, geostatistics, etc.), performance warnings are sent to the operations team by e-mail to initiate ad hoc countermeasures. In very rare cases, these countermeasures can also cause a short downtime.

3.4 Backup and restore

3.4.1 Backup

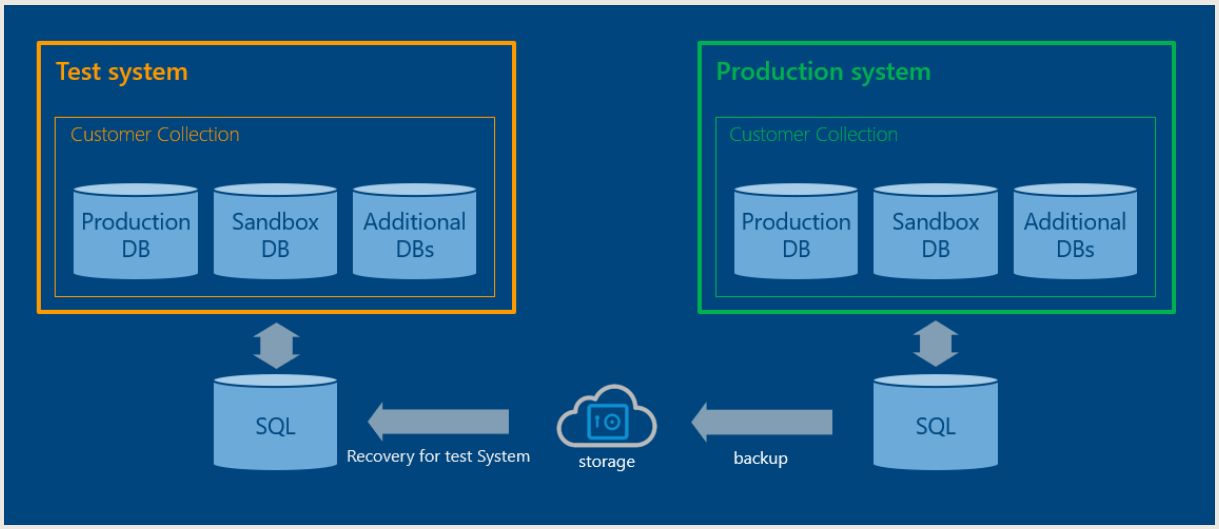
- Azure SQL
  - All Symbio data is saved in SQL databases.
  - Databases are saved regularly:
    - Full backup weekly
    - Differentially every 4 hours
    - Transactions logs every 5-10 minutes
  - Database backups are kept for 35 days.
  - Database backups of databases that have been deleted are permanently deleted 35 days after deletion of the database.
  - Databases and their backups are encrypted.
    For encryption, the Transparent Data Encryption (TDE) procedure is used with TDEs managed by the service. Details on this procedure can be found under the following link:
    https://aka.ms/sqlazuretde
- Application Server
  - There is no customer data on the application server, except log data.
  - Virtual machines are backed up at night at 2 a.m.
  - The hard disks are encrypted with BitLocker (AES 128 bit).

3.4.2 Restore

Database restores are possible after consultation or are carried out by the operation team in case of fatal errors. If a restore of your data is necessary, you will be informed in advance.

3.4.3 Recovery tests

Recovery tests are performed approximately every 8 weeks (per Symbio release) as part of an upgrade. The data is replicated from the Prod-System into the Test-System. This procedure checks cyclically that the backups function without errors.



3.5 Update/upgrade to newer versions

When are updates/upgrades run?

3.5.1 Hotfixes and updates

Hotfixes are imported automatically during the maintenance windows. The times for the maintenance window are defined in the SLA contract.

3.5.2 Upgrades

Version upgrades are available approximately every 8 weeks. In the standard cloud, upgrades are automatically installed during the maintenance window. In the Exclusive-Cloud, these will be recorded by arrangement.

3.6 Relocate/database operations

3.6.1 Copying of a Production database (sandbox)

It is generally possible to provide a copy of your productive database in Symbio. Please contact us for more information.

3.7 Privacy and Security Settings

3.7.1 Application Server

The operation team accesses the application server. This is only possible by filling out a JIT-Access request. The request can only be generated by an authorized user from our organization with the required rights. In order to generate a request the user has to log into his Microsoft account, which is secured by 2FA, access the JIT board and fill out the form. There he has the option to allow traffic from a specific IP over a specific port for a specific ammount of time (up to 9 hours).
Access to the actual server is realized via local users with predefined password.

3.7.1.1 Database authentication (Azure SQL)

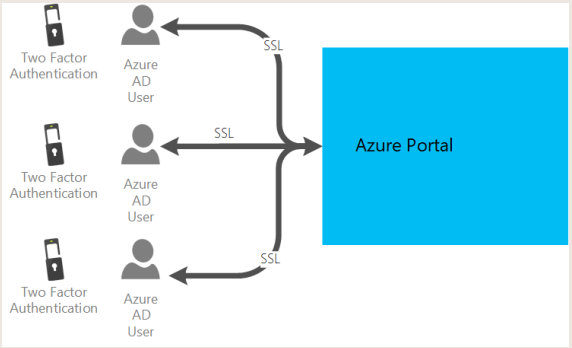
Authentication between the application server and Azure SQL is performed by Azure AD users. No passwords are stored in plain text on the application server. A separate user is used for each Symbio instance.

3.7.1.2 Encryption of the hard disks

The hard disks are encrypted with BitLocker (AES 128 bit).
https://azure.microsoft.com/documentation/articles/storage-service-encryption/

3.7.2 Azure portal (incl. Azure Services)

The Azure Portal is accessed by the Operations Team. Accesses are personalized via Azure AD. The corresponding Azure AD users are secured with multi-factor authentication. On trusted devices, multi-factor authentication must be renewed after 30 days.
The passwords of Azure AD users are renewed after 180 days.



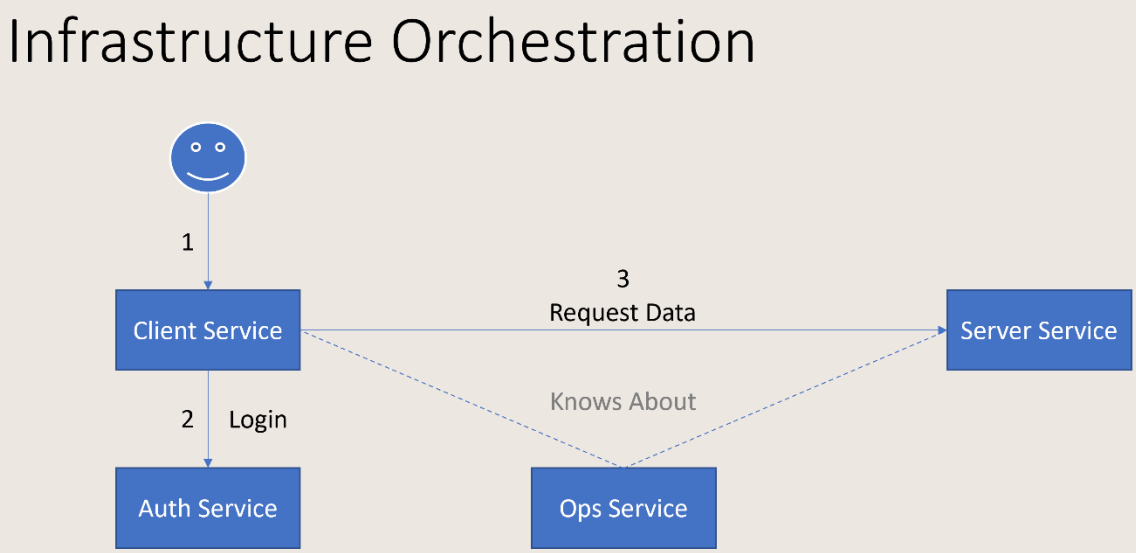
3.7.3 Symbio access

All Symbio users are authenticated via single sign-on via SAML.

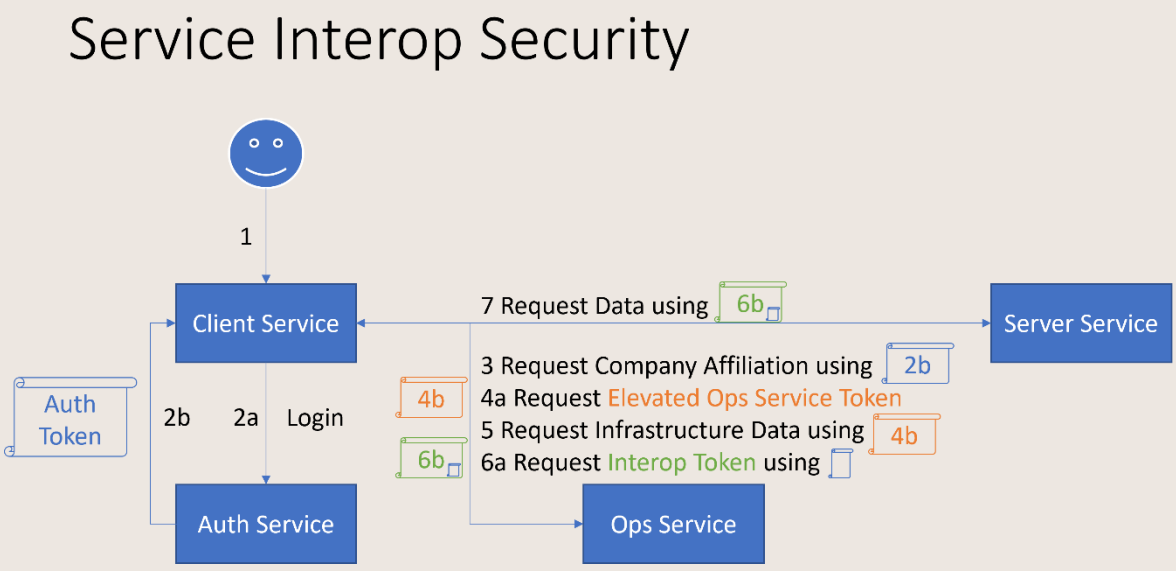
In the same way, Symbio Consultants can also access the data after consultation with the customer.
This ensures that all connections between client and server are SSL encrypted
For more details please see online documentation.

3.7.4 Inter-Service (Interop) Security

Services in the Symbio ecosystem are orchestrated by the Symbio Operations Service (Ops Service) that knows about them and the context in which they may be used:



While the user login to an application is facilitated by the Symbio Authorization Service (Auth Service), the communication among services is secured by the Ops Service. This is especially true for services providing access to confidential data (in contrast of processing only provided data):



Three kinds of tokens are involved in securing application/service acces:

- **Auth Tokens** identify a user and are handed out during user login
- **Elevated Ops Service Tokens** identify a service and can be requested by a service to request/manipulate infrastructure data in the Ops Service that cannot be normally accessed by typical user
- **Interop Tokens** indetify a user in the context of inter-service communication and can be requested by a client service for a specific user and target/server service; this token is only issued when the target service may be accessed and the target service will be able to identify the associated user and apply any service-specific permissions

These tokens are JSON Web Tokens (https://jwt.io/) and are issued based on OpenID Connect and OAuth2 principals.

Symbioworld GmbH
Einsteinring 41-43
85609 München
Tel.: +49 89 890635 – 0
Fax: +49 89 890635 – 55
E-Mail: info@symbioworld.de

Imprint
Symbioworld GmbH assumes no liability for the correctness and completeness of the representation/illustration in the document. The described and possible functionalities of the software refer to the current version. Customer-specific adaptations are not included. The information in this document may change at any time. Symbioworld GmbH is not obliged to inform about updates of the document.