WHITE PAPER

STP Cloud

Security Technical Whitepaper

Confidential

Content

1 What is STP Cloud?

The Cloud allows global accessibility, instant collaboration, almost limitless scalability and reduced IT costs. We believe in the future of the Cloud. We also believe in protection of professional secrets and lawyer compliance. This is why we at STP strive to create solutions to address both. With the STP Cloud we offer functionality to extend our solid on-premises Software with selected features in the Cloud, without compromising on lawyer compliance. That enables law firms to take advantage of cloud benefits for specific use cases and to still rely on core data to be stored on-premises.

1.1 Objectives

In this document we write about decisions and features that enable and support the security of the STP-Cloud. We want to be as transparent as possible and help you understand our efforts to provide highest security and protection of data in the STP-Cloud.

1.2 Mission Statement

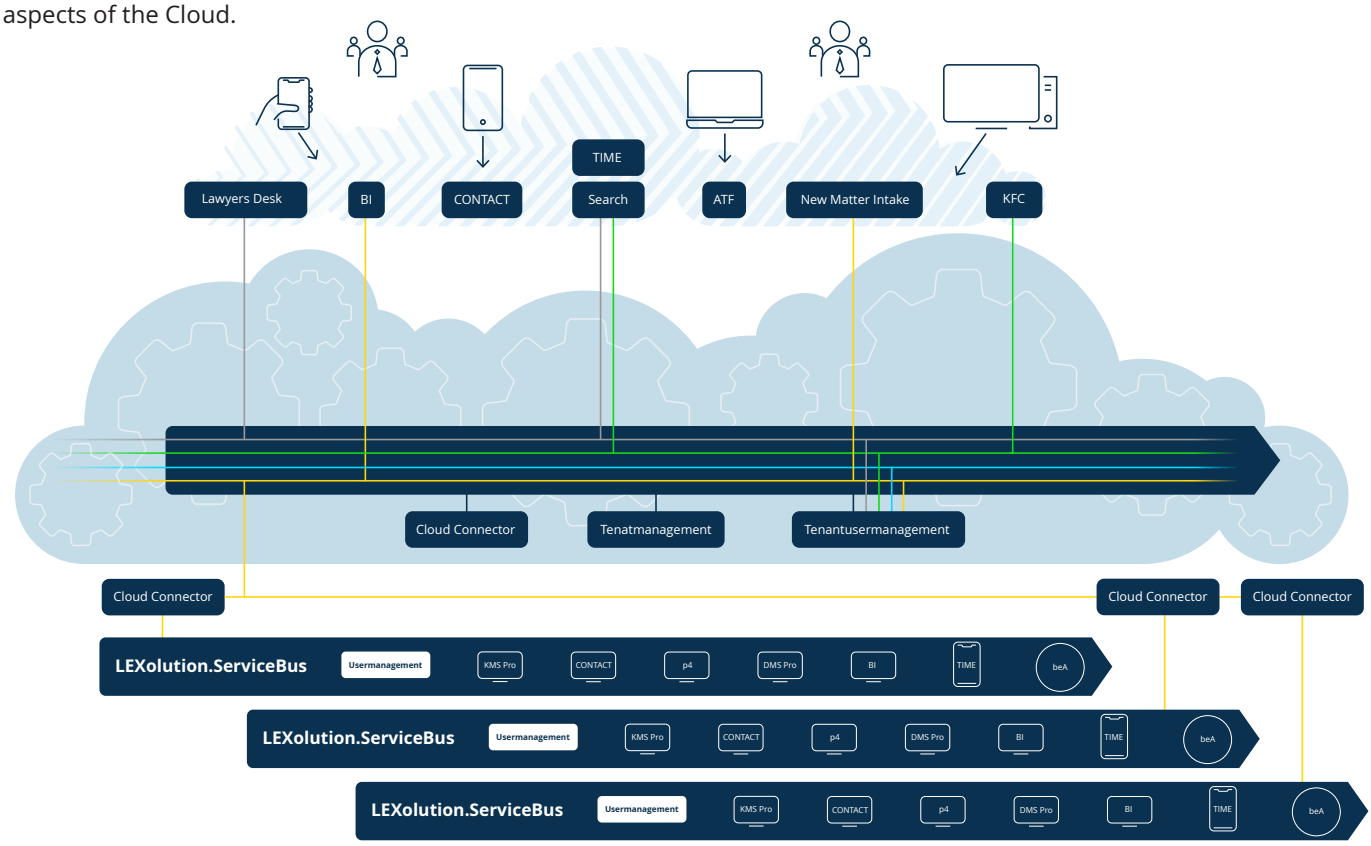
Our mission is to enable lawyers to take advantage of modern technologies. The Cloud is the perfect runtime for many business processes already and will continue to modernize all industries. Law firms, legal departments and individual lawyers have special requirements on cloud services. In order to remain compliant not every cloud offering can be used. We know about lawful compliance and security requirements, so we developed a platform and continue to do so, that lets you take advantage of many aspects of the Cloud.

STP offers on-premises Software that stores data securely on your servers. At the same time we want to enable your processes and agile services. We built a platform over which you can offer your customers additional services. Those services and processes can span over multiple parties where not all participants are residents in your IT landscape. The Cloud provides the perfect infrastructure for that. Your on-premises Software still is the central data storage facility. It supplies cloud-based processes and services to increase the functionality of your overall practice. We just provide the platform for your services. We believe this combination to be the best way to still have secure on-premises and yet to benefit from Cloud potential.

1.3 Principal architecture of STP Cloud

With the architecture of the STP Cloud we will combine the power of the LEXOLUTION Products installed on-premise on site at our clients with the easy access to workflows and information for the lawyers on a web based front end without media brakes. Data storage and control is done by the on-premises installed LEXOLUTION products. Data usage in the Cloud is only on a cached basis, to show e.g. searched information or the information which is needed to trigger a workflow. Additional information entered by the client can also be stored in the cloud. This combination of Cloud and on-premises solutions is unique in the legal tech market in Europe.

The following picture shows
the principal of the STP Cloud:



2 Managed Cloud Services from gridscale

As of May 2019, there are several competitive CSP's (Cloud Solution Provider) on the market offering a similar portfolio in regard to technical features, resources and availability. Whilst the big three – Amazon Web Services, Microsoft Azure and Google Cloud Platform – all fulfil the demands from a pure technical point of view, but none of them can guarantee that the data is protected from access by the provider's home country. In this case, the C.L.O.U.D Act allows the USA to force the release of the data. To prevent this from happening can only be guaranteed by a provider within the EU, which is subject to the corresponding data protection laws. STP complies with this in particular by selecting a German managed cloud provider for hosting the cloud, with redundantly separated locations in both Switzerland and as well in Germany.

The provider gridscale is equipped with all corresponding certificates (Link: https://gridscale.io/sicherheit/) and has additionally committed itself to STP by signing a special agreement concerning confidentiality obligation in § 203 StGB and § 43e BRAO of our customer and STP. Also see: https://www.trusted-cloud.de/de/cloudservices/2566/gridscale-public-paas

For STP data security is the number one priority preventing unauthorized access to customer data at all cost by fully leveraging and implementing the security concepts offered by Azure Germany. As the escrow agreement states, all customer data remains on servers inside a German data centre, or as well in the Swiss data centre at all time. A key feature of employed data trust principle is that the data trustee operates under German law and Swiss law if using the Swiss Cloud offering.

With the „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen"[1], entered into force on November 2017, lawyers are enabled to use remote computing services and cloud service providers without being liable as a principal. In order to be compliant Lawyers have to carefully select service providers[2]. If the service is provided outside of Germany, the protection of professional secrets in the other country has to be comparable to the protection of professional secrets in Germany[3]. We believe this to not be the case with any American cloud solution provider since the C.L.O.U.D. Act.

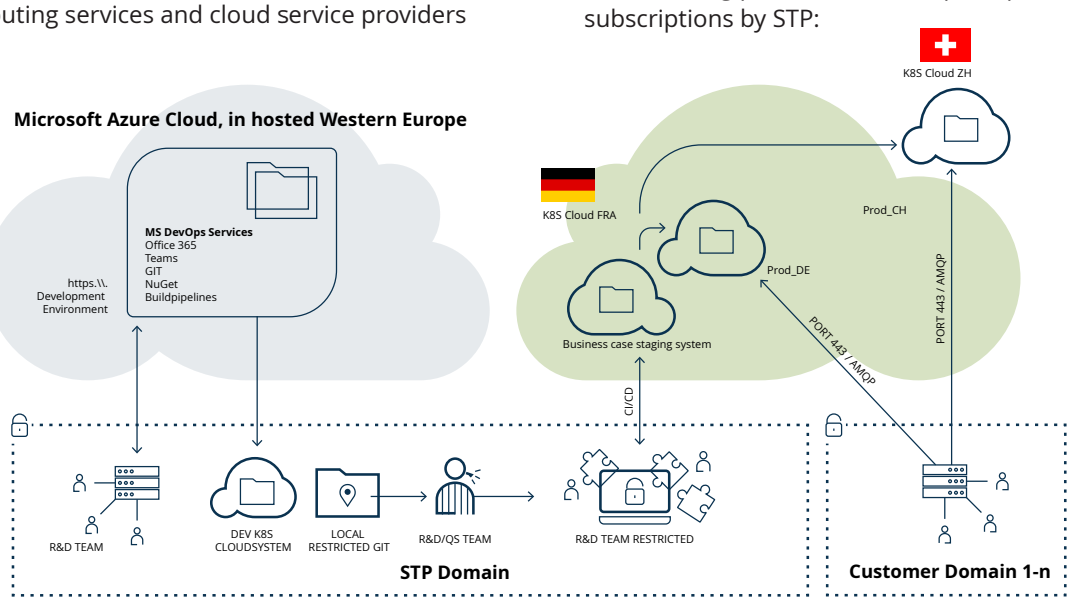
With the C.L.O.U.D. Act rendering into force on March 2018, the American government can legally compel any "provider of electronic communication service or remote computing service" to "disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." [4]

We understand that means that as long as the Cloud Solution Provider is bound by American law, which every CSP with an American parent company is, it can be compelled to disclose data regardless of where is resides, even if it is stored outside the US like Germany. If the German government enters into an executive agreement "under section 2523"[5] with the US, "MOTIONS TO QUASH OR MODIFY"[6] apply, allowing the CSP to reject disclosure. We are not aware of any executive agreement between Germany and the US and therefore cannot rely on American companies as data trustees.

gridscale GmbH offers high scalable secure managed cloud services with hosted georedundant data centers in Germany and Switzerland. That means we get all benefits of a modern managed cloud offering without the risks of the C.L.O.U.D. Act.

We use Microsoft Azure International only for development and testing purposes. We only use Germany and Switzerland hosted data centers for the publicly accessible STP-Cloud.

The following picture shows the principal of the used cloud subscriptions by STP:



3 On-premises data in the Cloud

On-premises are physically isolated by default. The STP Cloud provides a shared platform for many law firms and/or legal departments. The ones that use STP Cloud are referred to as tenants in this chapter. All data used in STP Cloud is strictly and closely bound to the tenant it belongs to. Not all data is solely generated in the Cloud. Some services can be supplied with data from on-premises to enhance functionality. That means that some data of your physically isolated systems is cached in the Cloud.

Each connector creates an encrypted queue to the Cloud. The encryption is done by ECC 256, which is a common standard (256 Bit ECC (Elliptic Curve Cryptography) encrypted messages over AMQP protocol (Recommended by BSI). The encryption is end-to-end and provides protection against man-in-the-middle attacks. The transport of the data is over TLS 1.2 with certificate.

4 Secure Application Development

We develop the STP Cloud with cross functional teams using the latest tools and technologies. Our Scaled Agile process enables multiple Scrum teams with highly specialized individuals to plan, develop, test and operate the platform. Each new feature is heavily tested automatically and manually, and has to be approved multiple times by different people in order to be prepared for deployment.

We develop the STP Cloud with a Cloud solution ourselves. We use Microsoft Azure DevOps[7] (Application Lifecycle Management Tool) and have compiles and tests run in the Cloud automatically on every change. All source code version control of STP Cloud is also hosted securely in Azure DevOps (Region West Europe). We don't commit passwords or access codes for production environments to the Cloud. If we need a secret in version control for an automated deployment, we encrypt it. A deployment agent then decrypts this secret on a machine in a secure zone on-STP-premise. All other secrets are securely version controlled in an on-premises repository, where only few selected people have access.

We never store any customer data outside of Germany or Switzerland (see Managed Cloud Services from gridscale)

5 Secure Operations

According to ITIL[8] methodology only few selected DevOps specialists are authorized to approve deployment of new versions of services to STP Cloud. That prevents data disclosure and no developer comes into contact with real life customer data. Security critical tasks in the continuous integration and continuous deployment pipeline, like the actual deployment into production clusters, are automated upon approval to prevent unintentional mistakes and security breaches.

Once a feature is deployed it is monitored by trained personnel to ensure optimal performance. All services take advantage of cluster load balancing, high availability and resilience. If a problem is found in one of the services, it is corrected and has to undergo the same testing and automated pipeline steps to eventually end up in production again.

While the clusters only host services for computational performance, data is stored on a scaled elastic SQL Server. All data governance, legal compliance and loss prevention features will be guaranteed by the Service Level Agreements of gridscale. That includes regular backups and transaction auditing.

The STP Cloud infrastructure itself can only be extended and administered by few specialized employees. These employees have been instructed and signed an extended confidentiality obligation to comply the specific requirements of the lawyers confidentiality according § 43e BRAO. All logins are personalized allowing transparent change history. Those accounts are further protected by Multi Factor Authentication.

6 BSI Catalogue

To make sure that our system (STP Cloud Applications) is secure, we use the BSI Catalogue to test and ensure our system against the actual items from the catalogue. Classical Hardware responsibilities for the Datacentre in Germany as in Swiss is handled by the cloud provider gridscale Germany.

0.1 Fire	Datacentre D/CH
0.2 Unfavourable Climatic Conditions	Datacentre D/CH
0.3 Water	Datacentre D/CH
0.4 Pollution, Dust, Corrosion	Datacentre D/CH
0.5 Natural Disasters	Datacentre D/CH
0.6 Environmental Disasters	Datacentre D/CH
0.7 Major Events in the Environment	Datacentre D/CH
0.8 Failure or Disruption of the Power Supply	Datacentre D/CH
0.9 Failure or Disruption of Communication Networks	Datacentre D/CH
0.10 Failure or Disruption of Mains Supply	Datacentre D/CH
0.11 Failure or Disruption of Service Providers	Datacentre D/CH
0.12 Interfering Radiation	Datacentre D/CH
0.13 Intercepting Compromising Emissions	Datacentre D/CH
0.14 Interception of Information / Espionage	SSL/VPN
0.15 Eavesdropping	SSL/VPN
0.16 Theft of Devices, Storage Media and Documents	Encryption
0.17 Loss of Devices, Storage Media and Documents	Encryption
0.18 Bad Planning or Lack of Adaption	Organization
0.19 Disclosure of Sensitive Information	Access Control/Encryption
0.20 Information or Products from an Unreliable Source	Process/Signature
0.21 Manipulation of Hardware or Software	gridscale/Process
0.22 Manipulation of Information	Signatures
0.23 Unauthorised Access to IT Systems	Password Policy
0.24 Destruction of Devices or Storage Media	Datacentre D/CH
0.25 Failure of Devices or Systems	Datacentre D/CH
0.26 Malfunction of Devices or Systems	Datacentre D/CH
0.27 Lack of Resources	Datacentre D/CH
0.28 Software Vulnerabilities or Errors	Monitoring
0.29 Violation of Laws or Regulations	Process
0.30 Unauthorised Use or Administration of Devices and Systems	Code
0.31 Incorrect Use or Administration of Devices and Systems	Code
0.32 Abuse of Authorisations	Code
0.33 Absence of Personnel	Business Continuity Planning
0.34 Attack	gridscale
0.35 Coercion, Extortion or Corruption	Organisation
0.36 Identity Theft	Code & Monitoring & Two Factor
0.37 Reputation of Actions	Process
0.38 Abuse of Personal Data	Code (Auditing, Lockout)
0.39 Malicious Software	Process
0.40 Denial of Service	gridscale, Code
0.41 Sabotage	Datacentre D/CH, Gridscale, Organization
0.42 Social Engineering	Process, Information, Education Coworkers
0.43 Replaying Messages	SSL
0.44 Unauthorised Entry to Premises	gridscale, Prozess
0.45 Data Loss	gridscale, Backup, Mirrors etc.
0.46 Loss of Integrity of Sensitive Information	Organization

7 Top Ten OWASP

OWASP Top 10[9] Most Critical Web Application Security Risks

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

STP checks by development, used tools, frameworks etc. to test and consider the newest OWASP Top 10 report.

STP development adopt this awareness document within their organization and start the process of ensuring that their web applications minimize these risks. Adopting the OWASP Top 10 is the most effective first step towards changing the software development culture within your organization into one that produces secure code.

Last report will adress the following points which will be tested by our QA and development:

A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with KnownVulnerabilities
A10:2017-Insufficient Logging & Monitoring

For more details and to get the latest report go to:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

1 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3618.pdf%27%5D__1512578315992

2 §43e (2) Bundesrechtsanwaltsordnung

3 §43e (4) Bundesrechtsanwaltsordnung

4 §2713, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

5 §2713 (1) (A) (i), https://www.congress.gov/bill/115th-congress/house-bill/4943/text

6 §2713 (2), https://www.congress.gov/bill/115th-congress/house-bill/4943/text

7 https://azure.microsoft.com/en-us/services/devops/

8 https://en.wikipedia.org/wiki/ITIL

9 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

STP Informationstechnologie GmbH

Brauerstraße 12 | 76135 Karlsruhe | Deutschland | Telefon +49 721 82815-0 | Telefax +49 721 82815-555

www.stp-solution.de