

HAUFE ZEUGNIS MANAGER AND AMAZON WEB SERVICES

Haufe Zeugnis Manager

Haufe Zeugnis Manager is the market-leading solution for creating employment references.

We are committed to providing our customers with the highest standards in terms of legally compliant content, product performance, and privacy.

For this reason, Haufe Zeugnis Manager will rely on the services of Amazon Web Services in the future.

AWS is already a proven partner of the Haufe Group for other products and has established itself as a reliable and secure service provider.

Therefore, in addition to technical precautions, we have also taken contractual measures to ensure the best possible security of your data.

This document provides you with a detailed insight into our technical measures for the protection of your customer data and is intended for use by data protection and information security officers.



Management Summary

The Haufe Zeugnis Manager relies on the services of Amazon Web Services EMEA SARL (AWS) as its hosting provider. The AWS data centers are certified according to the security standards DIN ISO/IEC 27001, 27017, 27018 and C5 certified. AWS meets the strictest security and compliance requirements and guarantees the highest stability and scalability of our infrastructure. All customer data is stored securely on servers within Germany (Frankfurt) and is encrypted both at rest and in transit. In addition, Haufe Zeugnis Manager implements comprehensive technical and organizational measures to ensure the security of data processing.

Compliance and legal matters



We chose AWS as our infrastructure partner after a careful selection process due to its security and compliance standards. AWS is certified to the internationally recognized standards ISO/IEC 27001, 27017 and 27018 and PCI DSS and is the first company to receive BSI C5 certification. A complete overview of all AWS compliance programs and certifications is available online.

Restriction of server locations to Germany



In order to meet data protection requirements, we have technically and contractually restricted the use of the services to Germany (EU-central-1 (Frankfurt)). The comprehensive data protection and IT security concept is based on the “Shared Responsibility Model”. AWS ensures the security of the cloud infrastructure, while we implement additional security measures.

Encryption



We use the AWS key management system (AWS KMS) to encrypt customer data. This system is designed in such a way that nobody can retrieve the encryption keys in plain text – not even the employees of AWS or Haufe. AWS KMS uses hardware security modules (HSMs) that are validated according to FIPS 140-2 to protect the confidentiality and integrity of your keys. The plaintext CMKs never leave the HSMs and are only used temporarily in memory. Software updates and firmware upgrades are subject to strict multi-party access control and are audited by a NIST-certified laboratory.

Monitoring



Every access and every use of AWS KMS keys is monitored and recorded, to detect unauthorized access. Access to the key management system is audited and checked for suspected security incidents. AWS KMS key rotation events are monitored in CloudTrail. In addition, we use Guard Duty, AWS Config and CloudWatch, which gives us comprehensive control of all activities in the infrastructure, enabling us to recognize and ward off threats.

Data separation in the context of encryption



The data is stored strictly separated between different AWS accounts. A KMS key from one AWS account cannot be used to encrypt or decrypt data in another account.

Transport encryption



The Haufe Zeugnis Manager systems always use transport encryption when data is transferred via insecure or public networks. The web interface and the API are only accessible via HTTPS connections, and client systems must use at least TLS 1.2.

Administrative access



Administrative access to the systems takes place exclusively via secure and authenticated connections. Haufe Zeugnis Manager uses AWS Identity and Access Management (IAM), which enables fine granulation of access to various services within the AWS cloud. IAM authorizations are provided automatically via SSO, and the “need-to-know” principle is strictly applied. Regular audits verify compliance with this principle.

Firewall and network separation



A web firewall is used to protect against common web exploits and bots. Different networks are separated by different AWS accounts and virtual private clouds (VPCs). Direct network access between VPCs in different AWS accounts is not possible.

Availability



Your data is stored exclusively in AWS data centers in Frankfurt am Main. All systems are redundant and distributed across several availability zones to ensure high availability.

Intrusion Detection



Haufe Zeugnis Manager uses a highly developed Intrusion Detection System (IDS) that analyzes log files, system files, login attempts, changes to permissions, network traffic. Known exploits are monitored. Security-relevant anomalies are automatically reported and critical anomalies such as rootkits are automatically prevented. The IDS supports security policy enforcement in accordance with PCI DSS 3.0.

Logging and audit trail



We use comprehensive logging for system events, error logging, user activities, logins and queries to database systems as well as security-relevant events. AWS CloudTrail enables the recording of all events within the cloud environments for forensic analysis.

Change management



System and software configurations are managed using “Infrastructure as Code”. Changes are tested in a staging environment before they are imported into the operating environment.

Backup



Daily backups of all necessary and customer data are performed to protect the infrastructure and customer data.

Performance



We use horizontal and vertical auto-scaling functions from AWS to optimize performance and adjust resources automatically.

Security audits



The security of the Haufe Zeugnis Manager application is regularly checked by external and internal audits in order to identify and eliminate potential weaknesses. With the Haufe Zeugnis Manager and AWS as a partner at our side, we offer you a secure, scalable and reliable solution for your certificates. Rely on our comprehensive security measures and benefit from the first-class performance and availability of our systems.