Technical documentation

Version: 2.0 from 10.02.2025

Slideroom GmbH
Business park Cité 4
76532 Baden-Baden

Phone: 07221 40 37 633
info@slideroom.de
www.slideroom.de

Grenke Bank AG
IBAN: DE21 2013 0400 0060 3067 27
BIC: GREB DEH1 XXX

VAT ID No. DE367213821
Local Court Mannheim
HRB 750 207

Managing Director:
Christian Vollmer
Maximilian Supper

Introduction

This documentation describes the architecture, security and operation of the PowerPoint add-in slideroom.

Note: This documentation is updated regularly to reflect changes to the architecture, security measures and other relevant information. It is reviewed and updated at least once a year or after significant changes to the application.

Overview of the application

- **Name of the application:** slideroom
- **Technology stack:** Vue.js with TypeScript in the frontend, Kotlin with Spring Boot in the backend, deployment via Gradle. Nginx as reverse proxy.

Technical documentation

1. Architecture

- **Database:** PostgreSQL for structured data and Microsoft Blob Storage for file storage.
- **Protocols:**
  - **HTTPS** for secure communication
  - **REST API** between frontend and backend as well as use of external REST APIs from Pexels and Pixabay (optionally selectable for users).

2. Security measures (pursuant to Art. 32 GDPR)

2.1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

Physical security / access control

- Hosting in Azure data centers in Germany. Highest security standard through Azure.
- No unauthorized persons on site: Access for authorized persons only.
- Alarm and video surveillance systems by the cloud provider.

Access control

- No unauthorized system use: secure passwords, automatic locking mechanisms, two-factor authentication.
- Encryption of data carriers on the development and administration devices.
- For our infrastructure: SSH only with key authentication (CTO and deputy only).

Access control

- Role-based access concepts within the application (currently user/admin) per organization.
- Developer/employee access to infrastructure only for necessary maintenance (need-to-know principle).
- Logging of all access to administrative systems.

Separation control

- Separate processing of data from different clients (multi-client capability).
- Separate development, test and production environments (sandboxing).

2.2 Pseudonymization (Art. 32 para. 1 lit. a; Art. 25 para. 1 GDPR)

- Uploaded files are stored pseudonymously so that no targeted search for content is possible.
- Personal data is only linked to separate references (IDs).
- Where possible and appropriate, data in the database is pseudonymized.
- Analytics tools only receive pseudonymized issue reports (if agreed).

2.3 Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

- Secure transmission via HTTPS/TLS
- Checksums are created for files which are then checked during retrieval to prevent manipulation.

2.4 Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Availability control

- Protection against data loss and failures: regular backups (every 4 hours) using Azure Backup.
- Firewall, virus protection, UPS in Azure infrastructure.

Rapid recoverability (Art. 32 para. 1 lit. c GDPR)

- Planned disaster recovery strategy (under development).
- Rollback mechanisms through regular backups.
- Versioning and soft delete at file level.

2.5 Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d; Art. 25 para. 1 GDPR)

Data protection management

- Regular checks of data processing processes, documentation and adaptation to current GDPR requirements.

Incident response management

- Notification of security incidents to clients and rapid response in accordance with defined processes.

2.6 Data protection-friendly default settings (Art. 25 para. 2 GDPR)

- Minimal data collection by default, opt-in for extended analyses.

Order control

- No forwarding or processing without instructions from the client (client = user within the organization).
- Strictly regulated selection of any sub-service providers (e.g. cloud providers).

3. Data flow and processing

Data collected

- **Personal data:** Name, e-mail and password (stored securely). Due to the necessary affiliation to an organization, the company affiliation is also indirectly known.
- **Usage data:** Login times and device information over the duration of the session. Optional opt-in for page views and click behaviour (pseudonymized).
- **Files and content:** Uploaded presentations and media and metadata.

Data storage

- **PostgreSQL:** Structured user data and metadata. Passwords and sensitive data are stored in encrypted form.
- **Microsoft Blob Storage:** Media content and presentations, accessible only to authorized users. In addition, the files are pseudonymized before storage so that no specific content can be searched for. Checksums are calculated and stored to prevent manipulation of the files.

Data processing

- **User registration and authentication:** via email/password or Microsoft SSO. Password processing by Spring Security and encrypted storage of the hash.
- **File management:** Files can be uploaded, saved and retrieved within the application.
- **Analysis and monitoring:** Page views and click behavior (opt-in), anonymized or pseudonymized (if agreed) error reports and logs to improve the application.

4. Authentication and authorization

Authentication

- **E-mail and password:** Password requirements (at least 8 characters, with special characters, number and capital letters).
- **Microsoft SSO:** Via OAuth2. After logging in, token and session processing takes place as with email authentication. The session information from Microsoft is only used to retrieve user data (during registration) and to authenticate the user and then discarded.
- **Multi-factor authentication (MFA):** Can be optionally enabled: either via email verification or TOTP (Authenticator app). Organizational policies to allow administrators to enforce MFA within an organization are planned.

Security mechanisms

- **Token security:** Tokens for session assignment are stored in HTTP-only cookies (Secure, HttpOnly and SameSite= Strict).
- **Device binding of tokens:** Internal mechanisms bind tokens to the respective device.
- **Session management:** Session timeouts for "Stay logged in" (1 year) or without (1 day). Auth cookies 5 minutes, for the refresh token ("Stay logged in") 1 year, otherwise "Session".

Authorization

- **Role-based access control:** Admin and user roles; future expansion planned. The administrator should be able to manage roles and authorizations.
- **Authorization check:** access control for every request; principle of least privilege.

5. Infrastructure

Hosting environment

- **Cloud platform:** Microsoft Azure in the Germany West Central region for German data protection regulations.

Network architecture

- **Virtual network (VNet):** One VM, no segmentation, NSG for traffic control.
- **Load balancer:** Currently not available, planned for future scaling.

Security measures for VMs

- **Operating system:** Ubuntu.
- **Access control:** SSH access with key authentication, only for administrators (CTO and deputy).

Availability and scalability

- **Scaling:** Currently vertical, horizontal scaling and load balancer planned for increasing load.

CI/CD processes

- **Build process:** Jenkins for builds and integration; only network access internally.
- **Deployment:** Manual deployment on production system, test system is deployed automatically.

Backup and disaster recovery

- **Backups:** Every 4 hours through Azure backup mechanisms.
- **Recovery:** Rollback possible in the event of problems through regular backups.
- **Disaster Recovery Plan:** Planned for future implementation.

6. Operation and maintenance

Updates and deployment

- **Update processes:** As required; extensive tests on a test system before deployment. Unit and UI tests are carried out during the build.

Supervision and monitoring

- **Monitoring tools:** Azure Alerts, bug tracking (Azure Application Insights) (opt-in for users possible).
- **Alerting:** Administrator is informed immediately in the event of critical conditions.

Access control and authorization management

- **Administrative access:** Strictly controlled, only CTO and representative.
- **Logging:** All accesses are logged for traceability**.**

Maintenance and security updates

- **Patch management:** Automatic updates for the operating system and application-specific features.

- **Security messages:** Administrator tracks security updates regularly (at least monthly). In addition, Azure responds immediately to security notifications.

7. Risks and measures

- **Unauthorized access to user data:** MFA, HTTPS encryption, password hashes with salt, limiting login attempts.
- **Cross-site scripting (XSS):** XSS protection through server-side validation of input. Escaping mechanisms from vue.js are used on the browser side.
- **Weak password security:** password requirements and feedback, optional MFA.
- **Man-in-the-middle (MitM) attacks:** HTTPS with TLS, HSTS for HTTPS enforcement, regular renewal of certificates.
- **SQL injection:** Use of JPA/Hibernate with parameterized queries, server-side validation.
- **Distributed Denial of Service (DDoS):** Rate limiting, planned use of Azure DDoS Protection Services (firewall).
- **Security vulnerabilities in third-party libraries:** Regular updates and security audits for external dependencies.
- **Data loss:** Regular backups and planned implementation of a disaster recovery plan.
- **Misconfiguration of the server:** Application of best practices, planned use of IaC tools.
- **Unauthorized access to administration interfaces:** Restricted access to admin functions and implementation of MFA for administrators.