Definitely a Trustworthy Investment

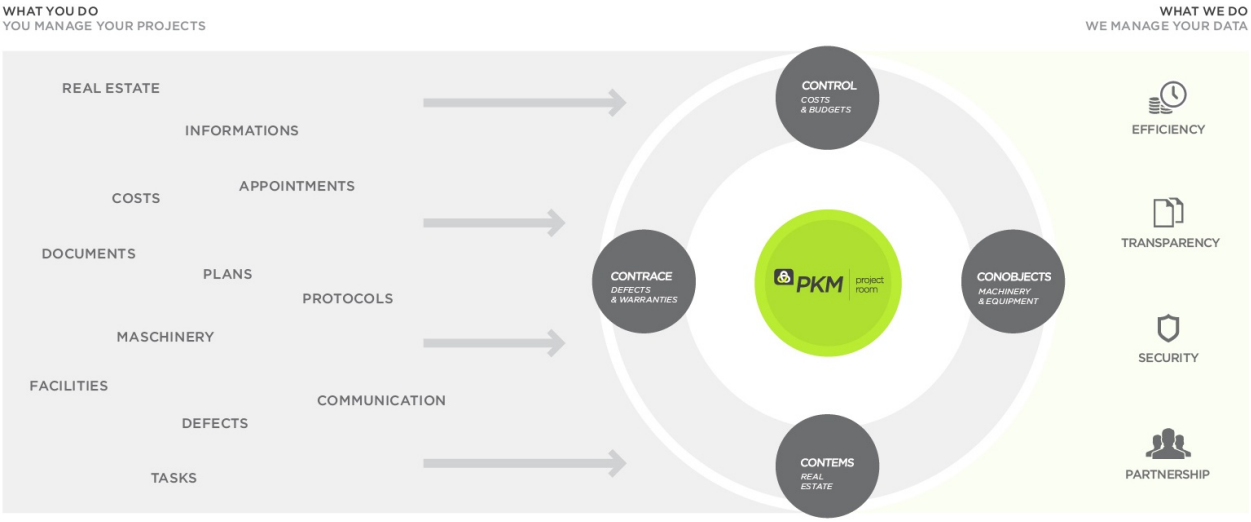
Physical and Logical Security of Conclude's SaaS Solutions

1. Introduction

Conclude GmbH offers solutions in a so called Software-as-a-Service (SaaS), meaning Conclude operates the solution on behalf of its customers and the customer only requires a standard PC with Internet access. The Conclude team handles operation of the software solutions, relevant servers, failure protection mechanisms, backups, virus protection and firewall management. The software applications are based on established Internet technologies and have perfected security mechanisms to protect your project data against unauthorized access, sabotage and theft.

The Conclude solutions not only offer efficiency and transparency, but also features comprehensive access protection and data security. After all, your project data deserves special protection. Many thousands of users in several hundred projects worldwide rely on the safety and security of our solutions and services.
The systems operated by Conclude are located at the high-security computer center KAMP in Oberhausen, Germany, with additional backup at the high-security computer center, myLoc in Düsseldorf, Germany – only 20 miles from the primary computer center KAMP.

The following pages detail the various security aspects, which uniformly apply to PKM, CONTROL, CONOBJECTS, CONTRACE and CONTEMS. Additional issues regarding logical security features within PKM are explained at the end of this paper.



Conclude GmbH · Ohligsmühle 3 · D–42103 Wuppertal
Telefon +49 202 – 693588–0 · **Fax** +49 202 – 693588–15 · **E–Mail** info@conclude.com

www.conclude.com

2. Physical Security

The Conclude servers are operated in Oberhausen at the KAMP computer center, which ranks as one of the most sophisticated co-location computer centers in Europe. Additional backups are managed in the computer center myLoc, in Düsseldorf. Access to the Conclude server infrastructure is limited to four full-time employees of Conclude, exclusively. Employees of the computer centers have no access at all. The servers run 24 hours a day 365 days of the year. Guaranteed availability of software, servers, and management averages 99 % in a typical year.

KAMP GmbH: Primary computer center

KAMP is one of the leading providers of high-availability co-location computer center infrastructures. The KAMP computer center features include:

- modern gas fire extinguishing systems
- state-of-the-art access authorization systems including alarm systems and physical security services
- redundant Internet connection employing backbones from various Internet providers
- dual power supply and backup power
- high efficiency, redundant air-conditioning systems

All this combined ensures an extremely high level of availability and data security.

The high-security areas are constructed as so called Lampertz cells, which are certified by the means of the European fire protection standard ECB-S (F180 / DIN 4102). KAMP is classified as TIER III by third party consultants. The computer center received an ISO 27001 certification in 2012. KAMP guarantees the physical security of the computer center by means of a three-stage security system providing surveillance of everything from the grounds outside and various buildings, to the rental spaces where the Conclude servers are located. Dual power supply and backup power supply ensure high level of reliability.

KAMP is family owned and managed by 2nd generation of family members.

KAMP Netzwerkdienste GmbH
Vestische Str. 89-91
46117 Oberhausen
Germany

myLoc AG: Backup computer center

The world's greatest Lampertz cell constitutes the core of the myLoc high-security computer center.

The myLoc computer center is equipped with:

- state-of-the-art fire extinguishing systems
- access authorization systems including alarm systems and physical security services
- redundant Internet connection employing backbones from various Internet providers
- dual power supply and backup power supply with an extremely high level of reliability.

myLoc is classified but not certified as TIER III by third party consultants. Conclude uses myLoc as data center for backups. In the rare case KAMP fails, myLoc can act as failover infrastructure within hours.

myLoc is a subsidiary of United Internet AG, which is listed in the TecDax.

myLoc managed IT AG
Am Gatherhof 44
40472 Düsseldorf
Germany

3. Technical Security

Secure Connection

To be able to use our software solutions only a modern web browser is required (e.g. Internet Explorer 7 or higher, Firefox) in which cookies and JavaScript are activated. In addition, uploading and downloading of files by means of the HTTPS protocol must be permitted by the firewall.

For data transmission, the tools use the encryption protocol SSL and with the aid of 256 bit encyption, message integrity is guaranteed between the user and the PKM server. After logging in each user is also given a session ID in order to ensure authenticity for the duration of the session. Because of this approach, the exchange of data with the server is much more secure than communication by email.

Firewall

Extensive protection is provided by a firewall. Continuous remote monitoring and updating by our experts ensures optimal protection against attacks from the Internet.

Antivirus Software

Conclude's software solutions are protected by a professional antivirus product. Updating takes place daily, on an hourly basis in some cases, and thus provides optimal protection against virus attack. All uploaded data is checked before it is stored. In addition, files with the following suffixes can not be uploaded to PKM for security reasons: *.bat, *.cmd, *.com, *.dll, *.exe, *.pif, *.scr, *.vb, *.wsh; however, settings can be customized to meet project-specific require-ments.

Logging

The logging system records user activity and covers the following:

- Every successful system login is retained in an auditing-proof manner. The username, date and time are recorded
- General file accesses (downloads, uploads, relocations)
- Changes in file names, comments, properties
- Internal project communication (emails received and sent, etc.)

CONTRACE defects & warranties

In addition, the activities and changes within the configurations executed by system or project administrators are also logged by the system.

4. Password Protected Access

The Conclude project tools are only available to authorized users identified by username and a valid password. Access to PKM is gained solely using encryption. Passwords are saved in the databases using SHA hash functions and cannot be read by anyone as plain text, including higher-level Conclude administration, in plain text. Tool and project specific access rights regulate the user's individual access privileges.

Administration Access

All the servers in Conclude's infrastructure are solely operated by Conclude and only four Conclude employees have direct access. Only Conclude employees know all infrastructure and application master passwords. Neither KAMP employees nor myLoc employees can access the server consoles.

Users can be given project-specific administration rights for a project. With project-specific administration rights a user can only set up and configure his/her particular project. Rights only relate to the respective project and its content. With such project-specific rights it is not possible to access other projects, meaning it is impossible to read data from third-party projects, administer other projects, or grant oneself administration rights.

Access Control and Password Restrictions

The creation of participants / users only takes place in agreement with our customer's authorized project leader. Various specifications can be implemented to ensure password complexity including dictonairy tests. In addition, settings can stipulate that the password has to be reset by the user at certain intervals. One can define which accounts may be used by which source IP addresses (IP restrictions).

CONTROL costs & budgets

When the user has logged in for the first time, he/she is requested to re-enter the password in order to change it according to the specified criteria. Rejected access attempts are also logged and if an incorrect password is entered several times, access is barred automatically.

5. Backups and Project Archiving

Local Backup at KAMP

Every backup takes place on dedicated backup servers that are located in a different rack with independent energy supply. All data backups use hard disks and not error prone data storage tapes.

Immediately after uploading, the files are copied to the backup. The databases are also backed up incrementally to the backup system every five minutes. A complete backup of the database is performed daily so a consistent state can be restored at any time.

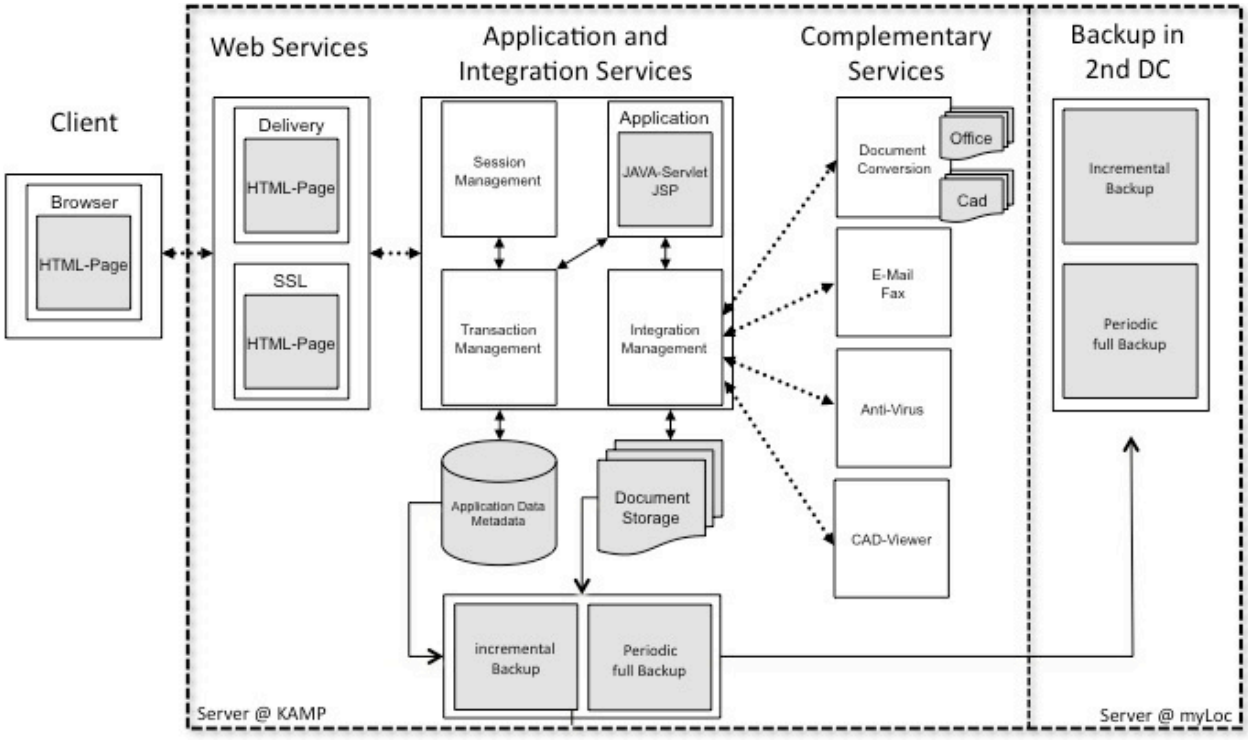
Distributed Backup at myLoc

In addition to the backup in the primary computer center a distributed backup of the database and files is stored in another location – the myLoc computer center in Düsseldorf. The distributed backup of the files is performed immedi-ately after the local primary backup and the distributed backup of the database is stored as an increment every five minutes. A full-backup of the database is transferred weekly to the distributed backup infrastructure at myLoc.

Consequently, myLoc functions as failover computer center as well.

Data Transfer after Project Completion
After project completion, the project documents, including meta information, is transferred to a suitable data storage medium. Alternatively the customer can also elect to continue to house project data on the PKM servers for a minimal fee.

The basic technical architecture of Conclude's SaaS-infrastructure is as follows:



6. Regular Security Tests

Conclude undergoes so-called "Penetration Tests" by objective, independent service providers and customers like the European Central Bank (ECB) and Deutsche Bank on a regular basis. Both the external and internal security of PKM is tested and validated.

The entire security test procedure, which is based on German Federal Office for Security in Information Technology standards checks amongst others the following protection mechanisms: Effectiveness of access control and authentication, checking of input fields, and session management with regard to misuse.

The regular tests are performed both with and without authorized user accounts, and with the aid of the following attack techniques: Dictionary attack, buffer overflow, SQL-, XSS- and JavaScript injection

7. Logical Security in PKM

The internet-based project room PKM networks all those involved in your project and serves as a central project platform. Drawings, documents, and information can be exchanged and managed with PKM securely.

In addition, our ServicePoint assists, and supports and protects the customer at project launch as well as all project participants, throughout the entire term of the project. In nearly all projects, the parties involved agree to use PKM as the legally binding data exchange and communications platform.

Documents cannot be deleted - if a document is uploaded to a folder already containing a file with the same file name or certain parts of the name, a version stack is created. As a result, documents can never be overwritten, replaced or deleted. Versioning of files is used to document the entire course of the project and protect against overwriting. In addition, it is impossible to delete files or remove them from the system. Depending on user permission configuration, documents can be shifted to the "recycle bin" and tagged "invalid", but they can never be completely deleted. It is not even possible for the administrator to empty the recycle bin.

Together with the logging system, document versioning ensures that project documentation integrity remains verifiable at any time.

Updated: November 2015

Conclude GmbH · Ohligsmühle 3 · D–42103 Wuppertal
Telefon +49 202 – 693588–0 · **Fax** +49 202 – 693588–15 · **E–Mail** info@conclude.com

www.conclude.com