Brief Description of Basic vitero Security Aspects

1 vitero Architecture

vitero's architecture is a client server architecture. **vitero** works with three servers. Each is specialized to fulfil different tasks.

User authentication is handled via a web server who counter-checks name and password with a user database. For application sharing a special server is used which is optimized for performant and encoded transmission of image data as well as input generated by keyboard and mouse. The transmission of so-called 'shared events,' video streaming and audio streaming (Voice over IP) is realized via another server (Adobe Media Server 5 Professional). For SaaS customers the audio connection is SSL-encoded by default. Shared events are events during a session that are executed for all participants simultaneously. Among them are the text chat but also actions such as the 'raise-hand' gesture or certain cooperative functions such as the launch of application sharing.

The user and data administration is realized via a web server connected to the database, the so-called Vitero Management System (VMS). For this purpose existing user databases which are, for instance, based on LDAP or Active Directory, can be connected as well.

The **vitero** client software does not need open ports for incoming connections as all connections are established by the client and, as a consequence, only the servers' replies are received. For out-going connections the ports 443 (https) and 16501 are needed. As an alternative to 16501, the ports 443 and 80 can be used.

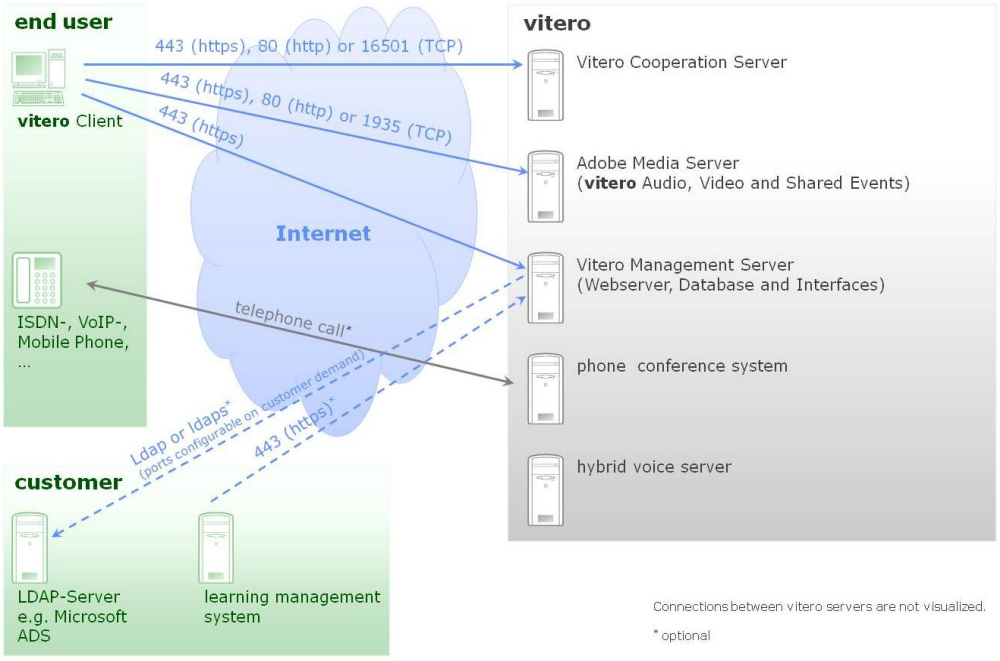

Fig. 1: **vitero** architecture (SaaS)

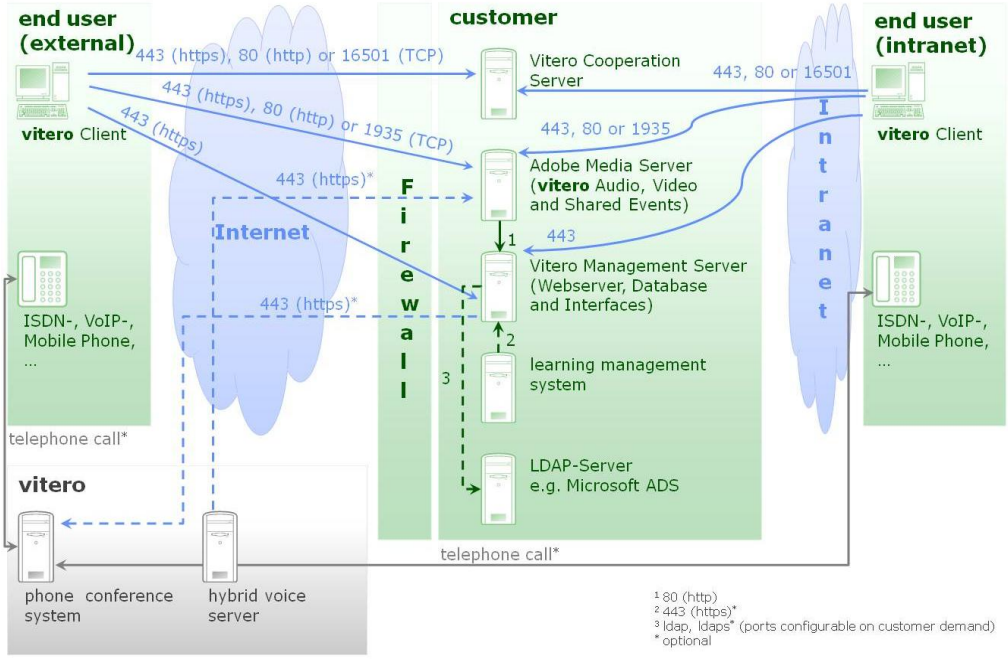

Fig. 2: **vitero** architecture (on premise)

2 Data Transmission Between Client and Web Server

The data transmitted between the client and the web server (Tomcat) are transmitted via a 128-bit SSL-encoded https connection. This technology is also used for online banking and state of the art in providing the ideal protection for data transmission to the web server. In this way, a protected channel is established between client and web server, through which the encrypted user specific data such as login information or booking information are transmitted. The same applies to documents used on the client for the **vitero** session, e.g., PowerPoint presentations stored on the server.

The database on the server is not open for access from the outside. The only way to access the database is via the web server. The database itself has its own special user account by which the web server has access to the database via a Java interface. This user account is password-protected and needs only the rights necessary to the tables needed by **vitero**. In this way, it has been taken care of that the database can only be accessed via the web server, i.e. via the VMS. For access, users have to successfully identify themselves, i.e. login into the system.

Via a conventional web browser (Internet Explorer, Firefox etc.) the VMS can be used to administer data, appointments and users. Again, https is used to encode the data transmission. Via the user login the respective user rights are defined so certain functions are only available for administrators.

3 Data Transmission between Client and Media Server

The clients do not communicate directly with one another but via the Adobe Flash Media Interactive server 4 or higher or Adobe Media Server 5 Professional. Via this server video- and audio streaming is realized as well as the transmission of events and statuses in the virtual session (shared events). These events and statuses in the virtual session, as well as the audio- and video streaming are transmitted via a 128-bit SSL-encoded https connection. In this way, the audio- and video connection is protected from eavesdropping, the text chat made safe from unauthorized read

along, and potential attackers are blocked from recording information such as attendance list, used gestures etc.

4 Data Transmission Between Client and Application Sharing Server

Application sharing means that the pictures displayed on a computer screen are transmitted to other computers. Additionally, it is possible to remote-control this computer. Between the clients there is no direct connection. The data are distributed by the server to the clients. At this point, a 128-bit blowfish coding is used. Each application sharing session can be identified by a unique session number. This session number is only known to the client software which the participants logged into the respective **vitero** session use. It's not visible for the participants. When a new session begins a new session number is generated. The application sharing server grants access to an application sharing session only if the correct session number is transmitted. In this way, only clients which have established a **vitero** session can access application sharing data.

5 Login With the vitero Client

5.1 Login Without Session Code

For login without session code, a **vitero** user account is required. In the course of logging in, user name and password are requested. They are transmitted in SSL code to the Tomcat server (see **2 Data Transmission Between Client and Web Server**), which in turn counter-checks the data with the user database. If the login process was successful the client is offered a list of session teams. In this way, it has been taken care of that a client can select only from teams for which it has the rights at the time of the login process. Access authorization depends on the license model as follows:

- **Access With Corporate Room/Corporate Café License**
  Team members without administration or team leader rights are allowed to enter booked rooms only.
  Team leaders are allowed to enter the room of their group without booking, but can only use it on their own then.
  Administrators can access the rooms of all teams regardless

whether they are a team member or an appointment has been booked. When the room is not booked administrators can use the room only on their own.

- **Access With Named Moderator License Without Session Code**
  A person-related room can be accessed by the group members only when the Named Moderator is present. Team leaders and administrators cannot use a person-related room on their own without the Named Moderator.

If login fails due to an unknown user name or an invalid password, the server has the client display an error message.

In the server configuration menu the maximum number of unsuccessful login attempts can be defined. If this number has been reached the respective user account will be locked. The server administrator can also define for how long the account will be locked, too. Optionally, a function to unlock the user account and to automatically generate a so-called password link can be activated through which the user in question can be given a new password.

The validity period of the password link depends on the setting made in the server configuration. If the link is used the user may create a new password. In addition, via the server configuration password rules can be activated in order the assist the user in choosing a secure password. If activated, the password is checked for certain criteria. These criteria are based on recommendations made by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) in their IT-Grundschutz-Katalog (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html). Among other things, criteria are applied in respect to the length of passwords (at least 8 characters), and selection of characters (combine letters, numbers and special characters).

To increase security even further, the validity period of password can be limited in the server configuration. If a user's password expires he is asked automatically to assign a new password when logging in.

5.2 Login With Session Code

For login with session code, a **vitero** user account is not required. Team selection is not required either, as the session code is assigned to a specific team.

With a Corporate Room License the session code can be generated **optionally** when booking the appointment in the Vitero Management System (VMS). It is only valid for this specific appointment.

With a Named Moderator license every person-related room has a permanent and stable session code. Login via session code is possible as soon as the Named Moderator is present in the virtual team room. In order to limit the range of authorized persons the Named Moderator may assign an additional session password which is only valid for the current session. The password becomes invalid when the Named Moderator leaves the session.

Notes:

If a session code is used then it is automatically added to the so-called direct session link. By clicking the link, the session code is automatically inserted into the login window of the **vitero** client.
Access with mobile devices is not possible without **vitero** user account, even if the direct session link contains a session code.

6 Confidentiality During a vitero Session

As all participants in **vitero** are represented by a clearly visible avatar (name and optional photo/live image) it is very easy to get an overview over all present participants. An exception to the rule is only possible when the module **vitero audience** is licensed (see annotations below). Due to participant representation by avatar, unwelcomed participants can be recognized easily and newly arriving participants perceived immediately. An unnoticeable 'sneaking' into a session is thus not possible.

Notes Concerning vitero audience:
vitero audience allows for the integration of spectators in a **vitero** session. The spectators are not represented by avatars but as a number in the gesture bar. Spectators with **vitero** user account can be given the respective role within a group in the VMS. Alternatively, a session code can be generated which allows for participation as a spectator without **vitero**

user account. When spectators are allowed during a session, participants in the virtual team room receive a note when they enter the room or change to an adjoining room and whenever a (new) spectator logs in.

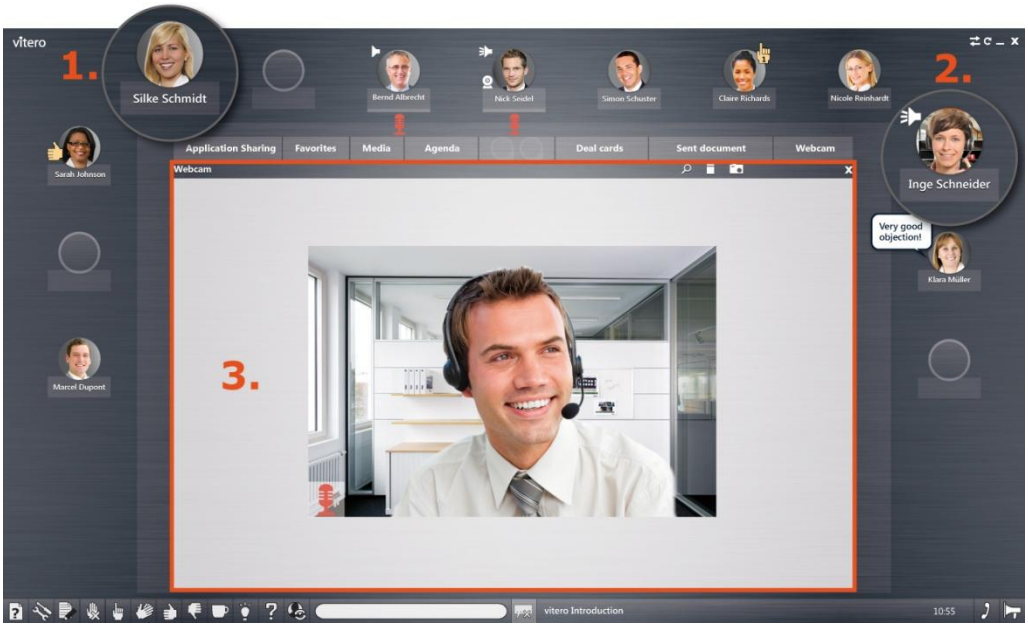

Fig. 3: Representation of participants in **vitero**:

1. Avatar with photo,
2. Avatar with live image,
3. Display of live image on the **vitero** desk

7 Security During Application Sharing

Security during application sharing is a decidedly crucial issue as the presenting person grants other participants insights into his own computer screen. Additionally, if the right for remote control is handed over the participant's computer can be remote-controlled with keyboard and mouse. An application sharing session is protected with a unique session number. These data are known only to the clients logged into the current session. They expire as soon as the last client has left the session. With the start of a new session a new session number is created.

The data (picture information and keyboard and mouse events) are themselves transmitted in code. A 128-bit Blowfish algorithm (see **4 Data Transmission Between Client and Application Sharing Server**) is used.

It is important for users to recognize easily whether and when data are transmitted during application sharing, and also who is able to view these data. For the presenter sharing his screen content it is also a matter of security to know at any time what other participants are able to view of his computer and who or if somebody has the right to remote-control his computer. In **vitero** this is realized with a few simple rules and thus easy to recognize for users. An application sharing session can always and exclusively be started by the participant whose screen content is supposed to be shared. It is not possible to view a participant's screen content without the participant's prior consent, i.e. he has to explicitly start application sharing function by mouse click. In this way, it has been taken care of that no user shares his screen content unless he actively contributes to this process.

Once the presenter has initiated an application sharing session, the requested application is displayed at the centre of **vitero**. This is also symbolized by the display on the virtual conference table (see Fig. 4). Everything that lies within the boundaries of this part of the presenter's screen is displayed to presenter and transmitted to the other participants, too. In this way, the presenter is fully aware of the contents shared with other participants as it is exactly the same as he can view himself (What You See Is What I See – WYSIWIS).

At the start of application sharing with a Windows PC the presenter can select from three different safety levels, so he can control what is transmitted via application sharing to other participants. With Apple Mac computers, the safety level selection is not available so that all open applications and the desktop are shared (level I).

By default, the safety levels are defined as follows:

- **Level I:** Other participants can view the presenter's desktop and all applications the presenter has opened.
- **Level II:** Other participants can view all applications the presenter has opened but not his desktop.
- **Level III:** Other participants can view only newly started applications that have been opened after application sharing. All other applications including the presenter's desktop are not transmitted.

Upon request the safety levels can be adjusted as desired by the customer (e.g., substitute or deactivate default safety levels, allow or prohibit certain applications). When a presenter wishes to end or pause temporarily the transmission of his screen contents he can do so quickly by clicking 'Close application sharing' (see Fig. 4); when **vitero** is minimized the transmission is paused temporarily. In this way, the presenter can switch quickly between applications meant to be shared and those which are not, without thinking twice.

For viewing participants the presenter's name is displayed in the menu bar of the application sharing and his avatar is depicted above the media display on the so-called moderator or co-moderator seat so it is always clear who is sharing his screen content.

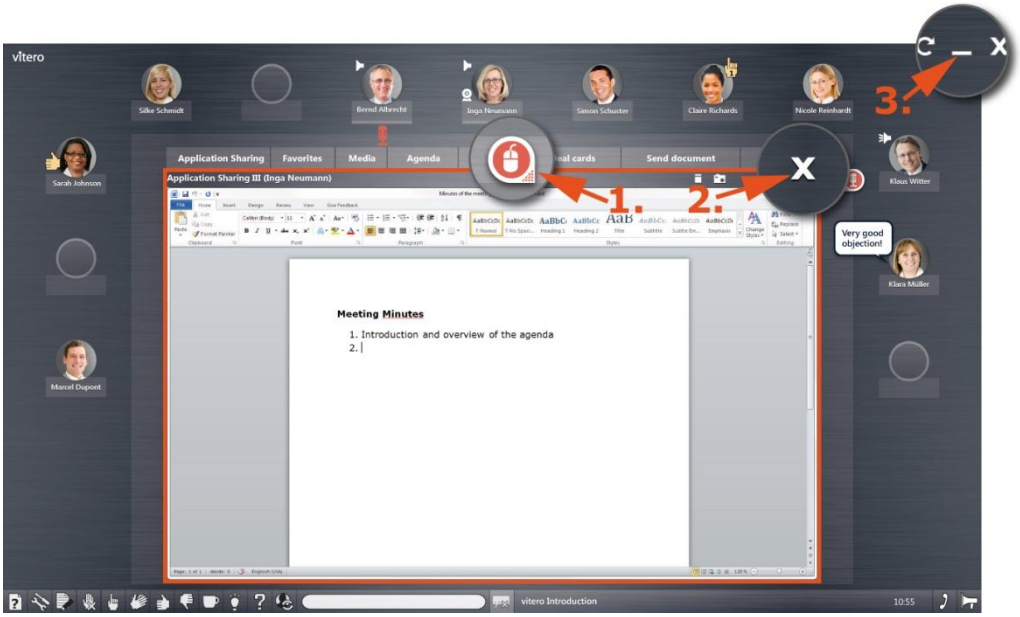

Fig. 4: **vitero** screenshot with opened application sharing
1. Virtual mouse (remote control),
2. Close application sharing,
3. Minimize **vitero**.

In case the presenter not only wants to show his screen contents but also wants to allow other participants to remote-control his local applications the presenter may grant a participant this right. The only person entitled to grant this right is the person who started application sharing. Other participants are not allowed to grant this right to themselves or to other participants. In this way, the presenter can always control who remote-controls his computer and when. In **vitero** the right for remote-control is symbolized by a virtual mouse. The virtual mouse is positioned at the participant's avatar who has the right for remote-control at the moment (relation of vicinity).

If the virtual mouse is positioned in the area between the function buttons then no other participant has the right for remote-control. In this way, it is immediately clear who has the right for remote-control.

In order to prevent malpractice through remote-control **vitero** has built in a number of security measures.

The extended keys (Fn keys on laptops) are exempt from transmission in order to prevent access on sensitive function of the target computer (e.g., brightness, open CD-drive, shut-down computer …).

The presenter may deactivate the remote-control function by pressing the Esc key. If the presenter is concerned that he might lose control over his computer he can deactivate the access for other people in a minimum of time.

Upon customer's request, the application sharing function can be deactivated either for the entire system or for certain customers, teams, roles, certain properties or types of sessions by order modification.