vitero Kurzdarstellung wesentlicher Sicherheitsaspekte

1 vitero Architektur

Die Architektur von **vitero** ist eine Client-Server-Architektur. **vitero** arbeitet mit 3 Servern, die für unterschiedliche Aufgaben spezialisiert sind.

Die Benutzerauthentifizierung erfolgt über einen Webserver gegen eine Benutzerdatenbank mit Name und Passwort. Für das Application Sharing wird ein spezieller Server genutzt, der für die performante, verschlüsselte Übertragung der Bilddaten sowie der Tastatur- und Mausereignisse optimiert ist. Die Übertragung der sogenannten Shared Events, das Videostreaming und das Audiostreaming (Voice over IP) erfolgt über einen weiteren Server (Adobe Media Server 5 Professional). Bei SaaS-Kunden ist die Audioverbindung immer SSL-verschlüsselt. Shared Events sind Ereignisse in der virtuellen Sitzung, die bei allen Teilnehmern gleichzeitig ausgeführt werden. Dazu gehört der Textchat, aber auch Aktionen wie Melden oder bestimmte gemeinsame **vitero** Funktionen, wie zum Beispiel das Application Sharing starten.

Die Benutzer- und Datenverwaltung erfolgt über einen Webserver mit Datenbankanbindung, das so genannte Vitero Management System (VMS). Hierfür können auch bestehende Benutzerdatenbanken auf Basis von beispielsweise LDAP oder Active Directory angebunden werden.

Die **vitero** Clientsoftware benötigt keine offenen Ports für ankommende Verbindungen, da sämtliche Verbindungen vom Client initiiert werden und daher nur die Antworten der Server entgegengenommen werden. Für ausgehende Verbindungen werden die Ports 443 (https) und 16501 benötigt. Alternativ zu 16501 können die Ports 443 und 80 genutzt werden.

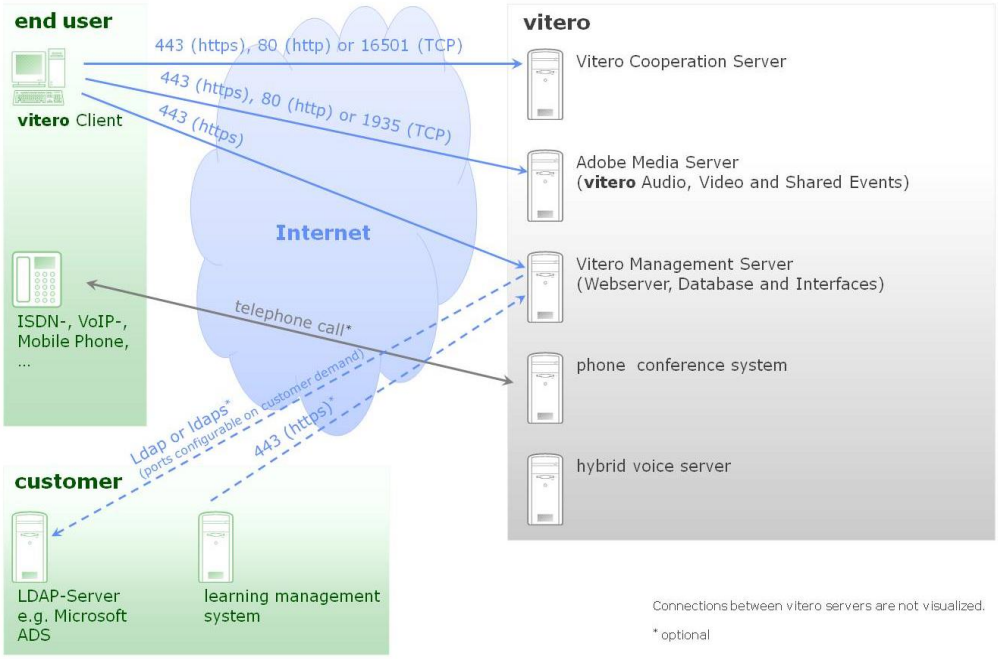

Abbildung 1: **vitero** Architektur (SaaS)

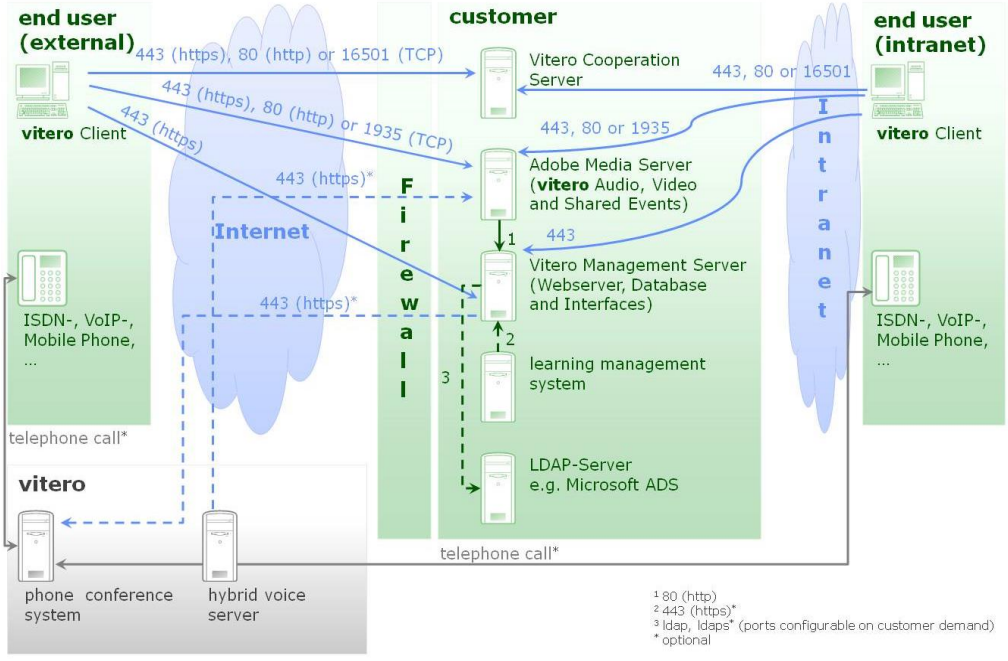

Abbildung 2: **vitero** Architektur (on premise)

2 Datenübertragung zwischen Client und Webserver

Die Daten, die zwischen Client und Webserver (Tomcat) übertragen werden, werden über eine 128-Bit SSL-verschlüsselte https Verbindung übertragen. Diese Technik, die z.B. auch beim Onlinebanking genutzt wird, bietet den nach aktuellem Stand der Technik optimalen Schutz für die Datenübertragung an den Webserver. So wird zwischen Client und Webserver ein geschützter Tunnel aufgebaut, in dem sowohl benutzerspezifische Daten wie Anmeldeinformationen oder Buchungsdaten, als auch für die **vitero** Sitzung auf dem Client benötigte Dokumente (z.B. auf dem Server bereitgestellte PowerPoint Präsentationen) verschlüsselt übertragen werden.

Die Datenbank auf dem Server wird nicht für Zugriffe von außen geöffnet. Der einzige Zugriff auf die Datenbank erfolgt so über den Webserver. Die Datenbank selbst verfügt über einen eigenen speziellen Benutzer, mit dem der Webserver über eine Javaschnittstelle Zugriff auf das Datenbanksystem erhalten kann. Dieses Benutzerkonto ist mit einem Passwort versehen und benötigt nur Rechte auf die von **vitero** benötigten Tabellen. Auf diese Weise ist sichergestellt, dass Zugriffe auf die Datenbank nur über den Webserver, also über das VMS erfolgen können. Benutzer müssen sich dafür erfolgreich am System identifiziert haben.

Über einen handelsüblichen Webbrowser (Internet Explorer, Firefox…) lässt sich das VMS zur Daten-, Termin- und Benutzerverwaltung verwenden. Auch hier kommt https zum Einsatz, um die Datenübertragung verschlüsselt zu sichern. Über die Benutzeranmeldung werden auch die jeweiligen Rechte des Benutzers definiert. So lassen sich bestimmte Funktionen nur von Administratoren ausführen.

3 Datenübertragung zwischen Client und Media Server

Die Clients kommunizieren nicht direkt untereinander, sondern über den Adobe Flash Media Interactive Server 4 oder höher bzw. Adobe Media Server 5 Professional. Über diesen finden sowohl das Videostreaming und das Audiostreaming statt, als auch die Übertragung von Ereignissen und Zuständen in der virtuellen Sitzung (Shared Events). Diese Ereignisse und Zustände in der virtuellen Sitzung, sowie das Audio- und Videostreaming werden über eine 128-Bit SSL-verschlüsselte https Verbindung übertragen.

Auf diese Weise werden die Audio- und Videoübertragung abhörsicher, der Textchat in **vitero** vor unbefugtem Mitlesen geschützt und mögliche Angreifer daran gehindert Informationen, wie anwesende Personen, ausgelöste Gesten usw., zu erfassen.

4 Datenübertragung zwischen Client und Application Sharing Server

Beim Application Sharing wird der Bildschirminhalt eines Rechners an andere Rechner übertragen. Zudem besteht die Möglichkeit diesen Rechner fernzusteuern. Zwischen den Clients findet keine direkte Verbindung statt. Die Daten werden vom Server an die Clients verteilt. Hier kommt eine 128-Bit Blowfish-Verschlüsselung zum Einsatz.

Die vitero-Clients bauen die Verbindung zum Server auf. Nach dem netzwerkseitigen Verbindungsaufbau sendet der Server ein X.509 SSL-Serverzertifikat, welches die „Echtheit" des Servers verifiziert.

Der darin enthaltene öffentliche RSA-Schlüssel (2048 bit) wird nachfolgend genutzt, um Daten verschlüsselt an den Server zu senden. Da nur der gewünschte Server in Besitz des zugehörigen privaten RSA-Schlüssels ist, kann nur er diese Daten dechiffrieren. Der Client sendet einen Sitzungsschlüssel an den Server, welcher auf Client-Seite mit Hilfe von anerkannten Zufallsgeneratoren (OpenSSL) erzeugt wurde.

Dieser Sitzungsschlüssel wird für die weitere symmetrische Verschlüsselung der Daten mit dem Blowfish-Algorithmus (128 Bit) verwendet.

Jede Application Sharing Sitzung ist über eine eindeutige Sitzungsnummer identifiziert. Diese Sitzungsnummer ist nur der Clientsoftware der in der entsprechenden **vitero** Sitzung angemeldeten Teilnehmer bekannt und wird nicht an den Benutzer ausgegeben. Bei jedem Sitzungsbeginn wird die Sitzungsnummer neu generiert. Der Application Sharing Server lässt Zugriffe auf eine Application Sharing Sitzung nur zu, wenn die korrekte Sitzungsnummer übertragen wird. Auf diese Weise können nur Clients, die eine **vitero** Sitzung aufgebaut haben auf die Application Sharing Daten zu greifen.

5 Anmeldung am vitero Client

5.1 Anmeldung ohne Sitzungscode

Für die Anmeldung ohne Sitzungscode wird ein **vitero** Benutzerkonto benötigt. Beim Anmelden werden Benutzername und Passwort abgefragt.

Diese werden SSL geschützt an den Tomcatserver übertragen (siehe **2 Datenübertragung zwischen Client und Webserver**), der die Daten mit einer Benutzerdatenbank überprüft.

Bei erfolgreicher Anmeldung wird dem Client eine Liste ihm zur Verfügung stehender Sitzungsgruppen übergeben. So ist sichergestellt, dass ein Client nur die Gruppenräume zur Auswahl hat, für die er zum Zeitpunkt der Anmeldung auch Berechtigungen hat. Die Zutrittsberechtigungen unterscheiden sich dabei je nach Lizenzmodell wie folgt:

- **Zutritt bei Corporate Room/Corporate Café Lizenzen**
  Gruppenmitglieder ohne Administrator- oder Gruppenleiterrechte dürfen nur die aktuell gebuchten Räume betreten. Gruppenleiter dürfen den Raum ihrer Gruppe auch ohne Buchung betreten, können ihn dann aber nur alleine nutzen.
  Administratoren können die Räume aller Gruppen betreten, unabhängig davon, ob Sie selbst Gruppenmitglied sind und ob ein Termin gebucht wurde. Ohne Terminbuchung können auch Administratoren den jeweiligen Gruppenraum nur alleine nutzen.
- **Zutritt bei Named Moderator Lizenzen ohne Sitzungscode**
  Ein personenbezogener Raum kann von den Gruppenmitgliedern nur betreten werden, wenn der Named Moderator anwesend ist. Auch Gruppenleiter und Administratoren können einen personenbezogenen Raum nicht alleine, ohne den Named Moderator betreten.

Falls die Anmeldung nicht erfolgreich durchgeführt werden kann, da der Benutzername unbekannt oder das Passwort nicht korrekt ist, veranlasst der Server den Client, eine entsprechende Fehlermeldung auszugeben.

In der Serverkonfiguration kann die maximale Anzahl der fehlerhaften Anmeldeversuche eingestellt werden. Ist diese erreicht, wird das entsprechende Benutzerkonto gesperrt. Die Dauer der Sperrung kann dabei ebenfalls vom Serveradministrator festgelegt werden. Eine Funktion zur Freischaltung des Benutzerkontos und zur automatischen Generierung eines sogenannten Passwortlinks, über den der betroffene Benutzer ein neues Passwort eingeben kann, ist optional einsetzbar. Die Gültigkeitsdauer des Passwortlinks ist dabei ebenfalls in der Serverkonfiguration einstellbar. Durch Aufruf des Links hat der Benutzer

die Möglichkeit ein neues Passwort anzulegen. Über die Serverkonfiguration können zudem Passwortregeln aktiviert werden, durch die der Benutzer bei der Wahl eines sicheren Passworts unterstützt wird. Dabei werden an das Passwort bestimmte Kriterien angelegt. Diese Kriterien orientieren sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in den IT-Grundschutz-Katalogen (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html). Es werden unter anderem Kriterien wie Passwortlänge (mindestens 8 Zeichen), und Zeichenwahl (Mischung von Buchstaben, Ziffern und Sonderzeichen) angelegt.

Um die Sicherheit noch weiter zu verbessern, kann auch die Gültigkeit von Passwörtern in der Serverkonfiguration festgelegt werden. Nach Ablauf der angegebenen Frist werden die Benutzer automatisch beim Anmelden dazu aufgefordert, ein neues Passwort anzulegen.

5.2 Anmeldung mit Sitzungscode

Für Anmeldung mit einem Sitzungscode wird kein **vitero** Benutzerkonto benötigt. Die Gruppenraumauswahl entfällt ebenfalls, da der Sitzungscode immer eindeutig einer bestimmten Gruppe zugeordnet ist.

Bei Corporate Room Lizenzen kann der Sitzungscode **optional** bei der Buchung im Vitero Management System (VMS) für den entsprechenden Termin angelegt werden. Er ist dann ausschließlich für diesen Termin gültig.

Bei Named Moderator Lizenzen hat jeder personenbezogene Raum einen fest zugewiesenen, dauerhaften Sitzungscode. Die Anmeldung per Sitzungscode ist möglich, sobald der Named Moderator im virtual team room anwesend ist. Um den zutrittsberechtigten Personenkreis einzuschränken, kann der Named Moderator ein zusätzliches Sitzungspasswort vergeben, das nur für die aktuelle Sitzung gültig ist. Die Gültigkeit erlischt, sobald der Named Moderator den Raum verlässt.

Anmerkungen:
Wenn ein Sitzungscode vorhanden ist, wird er automatisch an den sogenannten Direct Session Link angefügt. Durch Klick auf den Link wird der Sitzungscode im Anmeldefenster des **vitero** Clients automatisch eingetragen. Der Zugang mit mobilen Endgeräten ist ohne ein **vitero** Benutzerkonto **nicht** möglich, auch wenn der Direct Session Link bereits einen Sitzungscode enthält.

6 Vertraulichkeit in der vitero Sitzung

Standardmäßig wird in **vitero** jeder Teilnehmer über einen deutlich sichtbaren sogenannten Avatar (Name und optional Foto/Livebild) repräsentiert. Eine Abweichung hiervon ist lediglich bei Lizenzierung des Moduls **vitero audience** möglich (siehe Anmerkungen unten). Durch die Darstellung als Avatar ist es sehr einfach, einen Überblick über alle anwesenden Teilnehmer zu gewinnen. So können ggf. unerwünschte Teilnehmer leicht erkannt und neu hinzukommende Teilnehmer sofort wahrgenommen werden. Ein unauffälliges „Hereinschleichen" in die Sitzung ist somit nicht möglich.

Anmerkungen zum Modul vitero audience:

vitero audience ermöglicht die Zuschaltung von Zuschauern zu einer **vitero** Sitzung. Die Zuschauer werden dabei nicht durch einzelne Avatare, sondern als Gesamtzahl in der Gestenleiste dargestellt. Zuschauer mit **vitero** Benutzerkonto können durch Vergabe der entsprechenden Rolle im VMS einer Gruppe zugeordnet werden. Alternativ kann bei der Buchung auch ein Sitzungscode angelegt werden, der die Teilnahme als Zuschauer ohne **vitero** Benutzerkonto ermöglicht. Sind Zuschauer in einer **vitero** Sitzung erlaubt, erhalten die Teilnehmer im virtual team room eine entsprechende Hinweismeldung, wenn sie den Raum betreten oder in einen Nebenraum wechseln und sobald ein (neuer) Zuschauer sich zuschaltet.

Abbildung 3: Darstellung der Teilnehmer in **vitero**:

1. Avatar mit Foto,
2. Avatar mit Livebild,
3. Anzeige des Livebilds auf dem Gruppentisch.

7 Sicherheit beim Application Sharing

Die Sicherheit beim Application Sharing ist ein besonders wichtiger Punkt, da der Zeigende den anderen Teilnehmern Einblick auf den eigenen Bildschirm gewährt. Wird das Recht zum Fernsteuern vergeben, kann zudem der Rechner von einem anderen Teilnehmer mit Tastatur und Maus ferngesteuert werden.

Eine Application Sharing Sitzung ist über eine eindeutige Sitzungsnummer gesichert. Diese Daten sind nur den in der aktuellen **vitero** Sitzung befindlichen Clients bekannt und verfallen, sobald der letzte Client die Sitzung verlassen hat. Bei Beginn der nächsten Sitzung wird die Sitzungsnummer neu erstellt.

Die Daten (Bildinformationen sowie Tastatur- und Mausereignisse) selbst werden verschlüsselt übertragen. Hierbei kommt der 128-Bit Blowfish Algorithmus (siehe **4 Datenübertragung zwischen Client und Application Sharing Server**) zum Einsatz.

Für die Benutzer ist es wichtig, einfach zu erkennen, ob und wann Daten beim Application Sharing übermittelt werden, und wer diese Daten sehen kann. Für denjenigen, der seinen Bildschirminhalt zeigt, ist es auch sicherheitsrelevant zu jedem Zeitpunkt zu wissen, was die Teilnehmer von seinem Rechner sehen können und ob bzw. wer den Rechner fernsteuern kann. Dies ist in **vitero** durch wenige einfache Regeln festgelegt und somit für die Benutzer leicht erkenntlich.

Eine Application Sharing Sitzung kann immer und ausschließlich nur derjenige starten, dessen Bildschirminhalt gezeigt werden soll. Es ist nicht möglich den Bildschirminhalt eines anderen Teilnehmers einzusehen, ohne dass dieser explizit per Mausklick die **vitero** Application Sharing Komponente selbst startet. Auf diese Weise ist sichergestellt, dass kein Benutzer ohne sein aktives Zutun den eigenen Bildschirminhalt Preis gibt.

Initiiert ein Benutzer eine Application Sharing Sitzung, wird in die Mitte der **vitero** Anwendung, symbolisiert durch eine Anzeigefläche auf einem virtuellen Tisch, die gewünschte Anwendung dargestellt (siehe Abbildung 4). Alles was sich beim Zeigenden innerhalb dieses Bildschirmbereichs befindet und für den Anwender sichtbar ist wird auch an die anderen Teilnehmer übertragen. Auf diese Weise ist sich der Zeigende immer im Klaren darüber, was die anderen von seinem Rechner sehen

können – genau das was er selbst sieht (What You See Is What I See: WYSIWIS).

Beim Starten von Application Sharing auf einem Windows PC stehen dem Zeigenden 3 Sicherheitsstufen zur Auswahl, über die er einstellen kann, was per Application Sharing an die anderen Teilnehmer übertragen wird. Bei Apple Mac Rechnern ist die Sicherheitsstufenauswahl nicht verfügbar, so dass immer alle geöffneten Anwendungen und auch der Desktop übertragen werden (Stufe I).

Standardmäßig sind die Sicherheitsstufen wie folgt definiert:

- **Stufe I:** Die anderen Teilnehmer sehen alle Anwendungen, die der Zeigende geöffnet hat und auch seinen Desktop.
- **Stufe II:** Die anderen Teilnehmer sehen bei dieser Einstellung zwar alle Anwendungen, die der Zeigende geöffnet hat, sein Desktop wird jedoch nicht übertragen.
- **Stufe III:** Es werden nur die Anwendungen übertragen, die der Zeigende neu öffnet, nachdem er Application Sharing gestartet hat. Alle Anwendungen, die bereits vor dem Starten von Application Sharing geöffnet waren, sowie der Desktop werden dabei nicht übertragen.

Auf Kundenwunsch können die Sicherheitsstufen angepasst werden (z.B. Substitution, Deaktivierung der vorgegebenen Sicherheitsstufen, generell bestimmte Anwendungen erlauben oder verbieten).

Möchte der Zeigende die Übertragung seines Bildschirminhalts beenden oder kurzzeitig unterbrechen, kann er dies mit einem Mausklick schnell durchführen. Die Übertragung kann über einen Mausklick auf den „Application Sharing schließen" Button beendet werden (siehe Abbildung 4) oder wird, wenn **vitero** minimiert wird, während dieser Zeit unterbrochen. Auf diese Weise ist es dem Zeigenden ohne weiteres möglich auch kurzfristig in andere Applikationen, die nicht gezeigt werden sollen, zu wechseln.

Für die betrachtenden Teilnehmer wird der Name des Zeigenden in der Titelleiste des Application Sharings sowie sein Avatar oberhalb des Inhaltsbereichs auf dem sogenannten Moderator bzw. Co-Moderatorstuhl deutlich dargestellt, so dass jederzeit erkennbar ist, wer gerade seinen Bildschirminhalt zur Verfügung stellt.

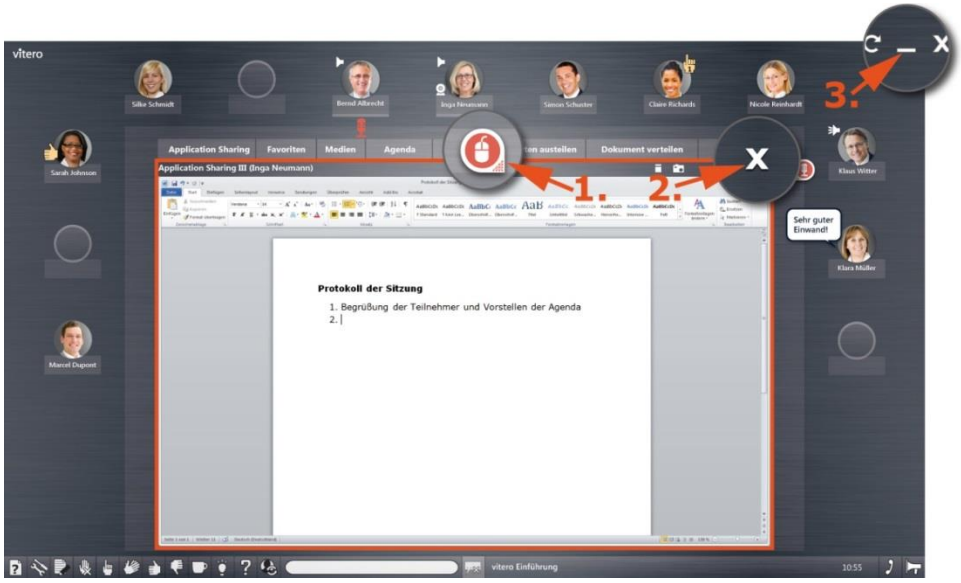

Abbildung 4: **vitero** Screenshot mit geöffnetem Application Sharing
1. virtuelle Maus (Fernsteuerrecht),
2. Application Sharing schließen,
3. **vitero** minimieren.

Um anderen nicht nur den eigenen Bildschirminhalt zu zeigen, sondern einen anderen Teilnehmer auch eine lokale Anwendungen steuern zu lassen, kann der Zeigende einem Teilnehmer das Recht gewähren seinen Rechner fernzusteuern. Dieses Recht kann nur derjenige vergeben, der die Application Sharing Funktion gestartet hat. Anderen Teilnehmer ist es nicht möglich sich selbst oder anderen dieses Recht zu gewähren. So hat der Zeigende immer die Kontrolle darüber, wer seinen Rechner zu einem bestimmten Zeitpunkt fernsteuern kann. Das Fernsteuerrecht wird in **vitero** durch eine virtuelle Maus symbolisiert. Diese virtuelle Maus wird am Avatar desjenigen Teilnehmers positioniert, der das Fernsteuerrecht zum jeweiligen Zeitpunkt hat (Näherelation).

Ist die Maus am Ablageplatz zwischen den Funktionsbuttons positioniert, so ist das Fernsteuerrecht keinem Teilnehmer gewährt. Auf diese Weise ist für jeden sofort ersichtlich, wer das Fernsteuern ausüben kann.

Um Missbrauch durch die Fernsteuerung vorzubeugen, sind in **vitero** mehrere Sicherungsmaßnahmen eingebaut.

Die extended keys (FN-Taste bei Notebooks) sind von der Übertragung ausgeschlossen, um zu verhindern, dass dadurch Zugriff auf schützenswerte Funktionen des Zielrechners genommen werden kann (Beispielsweise verändern der Bildschirmhelligkeit, Öffnen des CD-Laufwerks, Herunterfahren des Rechners …).

Der Zeigende hat die Möglichkeit über die ESC Taste auf seiner Tastatur mit einem Tastendruck die Fernsteuerung sofort zu deaktivieren. Dadurch kann er, wann immer er die Befürchtung hat die Kontrolle über den Rechner zu verlieren, in kürzester Zeit den Zugriff durch andere Personen deaktivieren.

Zusätzlich kann auf Kundenwunsch die Application Sharing Funktion für das gesamte System oder aber lediglich für bestimmte Mandanten, Gruppen, Rollen, Eigenschaften oder Sitzungstypen per Auftragsanpassung deaktiviert werden.