Ende-zu-Ende-Verschlüsselung mit Zoom

Autor: Marten Richter
Überarbeitung/Korrekturen: Erhard Zorn
Ergänzungen: Michael Flachsel
Ergänzungen aus Datenschutzsicht: Annette Hiller
Stand: 05.02.2021

Was bedeutet Ende-zu-Ende Verschlüsselung bei Zoom?

Bei Meetings und Webinaren bei Zoom werden die Audio/Video Daten **grundsätzlich verschlüsselt**. Bei der Standardverschlüsselung liegen die Schlüssel dazu in der Cloud bei Zoom, bei Veranstaltungen mit erhöhten Schutzbedarf ist hier ggf. ein erhöhtes Schutzniveau gefordert.

Bei der sogenannten **Ende2Ende** Verschlüsselung liegt dagegen der Schlüssel im Zoom-Client beim Host, welcher die Schlüssel an die Teilnehmenden über ein kryptographisches Verfahren (siehe End-to-End Encryption for Zoom Meetings) abgesichert verteilt. Damit sind nur die Teilnehmenden eines Meetings im Besitz der Schlüssel für das Meeting. Damit ist ein Zugriff von außerhalb auf den Meeting-Inhalt im Prinzip ausgeschlossen und erfüllt damit die Erfordernisse von Meetings mit erhöhtem Schutzbedarf.

Meetings, in denen vertrauliche Daten ausgetauscht werden (z.B. Bewerbungsgespräche, Prüfungen, nicht-öffentliche Gremiensitzungen, vertraulicher Forschungsaustausch) dürfen nur unter Verwendung der Ende-zu-Ende-Verschlüsselung durchgeführt werden. Bei Rückfragen wenden Sie sich bitte an das Präsidium oder das Team Datenschutz.

Für (Lehr-)veranstaltungen, die im Prinzip universitätsöffentlich oder öffentlich sind, also wo die Zugangsdaten einem breiten Teilnehmendenkreis zugänglich sind, bietet die Ende-zu-Ende-Verschlüsselung keine wirklich zusätzliche Sicherheit. Hier ist die Kenntnis der Zugangsdaten der schwächste Punkt in der Sicherheit dieser Meetings.

Welche Nachteile hat die Ende-zu-Ende Verschlüsselung?

Bei Verwendung der Ende-zu-Ende-Verschlüsselung ist eine Entschlüsselung in der Cloud von Zoom nicht möglich. Daher können folgende Dienste, die eine Entschlüsselung in der Cloud voraussetzen, prinzipbedingt **nicht verwendet** werden: Teilnahme über **Telefon, SIP/h323** (betrifft die Hardware in den Hörsälen H 0104, H 0105, H0107, H0110, EW 201, C130)**,** Live-Streaming .

Derzeit ist auch die Verwendung des **Webclients nicht möglich;** wir hoffen, dass sich dies ändert.

Folgende sonstige (auch für die Lehre wichtige) Funktionen an der TU Berlin sind im Moment bei Ende-zu-Ende-Verschlüsselung **nicht möglich**:

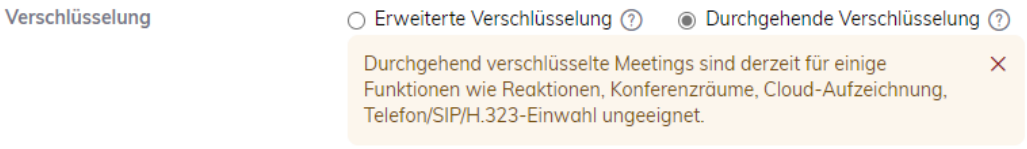
- Breakout-Räume,
- Umfragen,
- private Einzelchats (Einschränkung entfällt ab Version 5.5.0)
- Meeting-Reaktionen (Einschränkung entfällt ab Version 5.5.0)

Wir gehen aber davon aus, dass die Einschränkungen dieser 4 Punkte bald nicht mehr bestehen werden.

Wie kann man die Ende-zu-Ende Verschlüsselung aktivieren?

Für jedes Meeting einzeln umstellen

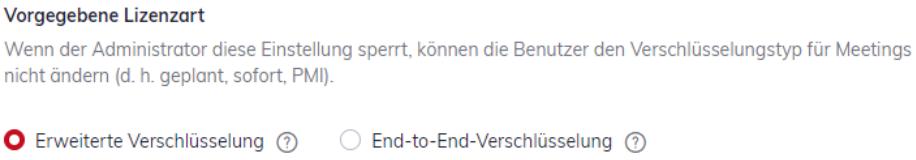
Sie müssen bei der Erstellung oder der Bearbeitung des Meetings **"durchgehende Verschlüsselung"** auswählen, (was Zooms Übersetzung für Ende-zu-Ende Verschlüsselung ist) :



Erweiterte Verschlüsselung bezeichnet die Standardverschlüsselung, bei der der Schlüssel in der Zoomcloud gespeichert ist.

Die Standardverschlüsselung für zukünftige Meetings ändern

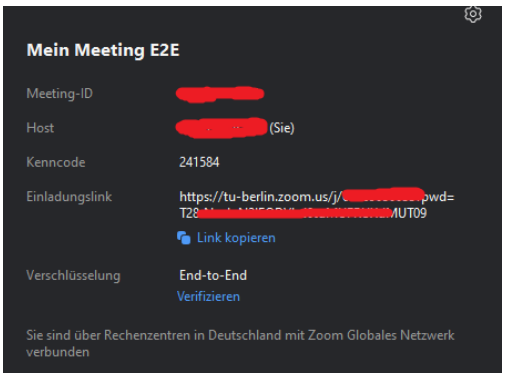
Gehen Sie im Zoom Webfrontend auf Einstellungen -> Meeting -> Sicherheit, dann finden Sie die Einstellung unter



Hierbei ist „Erweiterte Verschlüsselung“ die normale Verschlüsselung und „End-to-End-Verschlüsselung“ die Ende-zu-Ende Verschlüsselung.
Die TU Berlin hat im Moment die erweiterte Verschlüsselung vorgegeben. Die TU Berlin behält sich vor, wenn die Nachteile der Ende-zu-Ende-Verschlüsselung weniger werden, diese als Voreinstellung zu wählen oder diese auch verpflichtend zu machen.

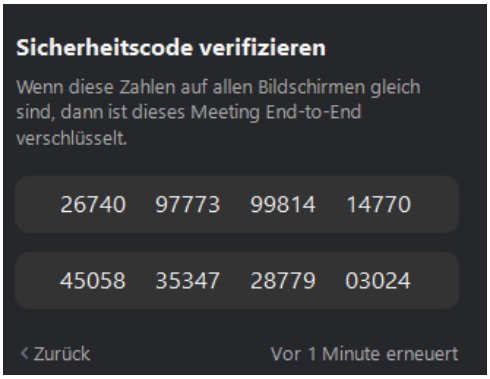
Wie kann man überprüfen, ob ein Meeting Ende-zu-Ende verschlüsselt ist und der Schlüssel sicher ist?

Im Meeting können Sie oben links auf das grüne Symbol klicken, dann sollten Sie Folgendes sehen:



Wichtig ist, dass unter „Verschlüsselung“ „End-to-End“ steht.

Unter Verifizieren können Sie dann einen Code ablesen:



Den lesen Sie am besten am Anfang des Meetings laut vor und die anderen Teilnehmenden schauen sich parallel ihren Code an; ist der Code bei allen identisch, ist kryptographisch gesichert, das niemand die Übermittlung der Schlüssel belauscht.