# Zoom Verschlüsselung

## Einführung

Zweck dieses Dokuments ist es, Informationen über die Verschlüsselungsmöglichkeiten für die Zoom-Plattform zur Verfügung zu stellen. Das Ziel unseres Verschlüsselungsdesigns ist es, ein Höchstmaß an Datenschutz zu bieten und dabei die unterschiedlichen Bedürfnisse unserer Kundenbasis zu unterstützen.

Es gibt mehrere unterschiedliche Anwendungsfälle und Möglichkeiten, wie ein Benutzer eine Verbindung zu Zoom aufbauen mag. Das folgende Dokument bietet eine Übersicht über die Verschlüsselungsmethoden, die von möglichen Schnittstellen zur Plattform verwendet werden.

# Wenn der Zoom-Client benutzt wird

Zoom bietet ein mit zahlreichen Funktionen ausgestattetes Client-Softwarepaket für Mac, Windows, iOS, Android und Linux, das eine Reihe von Verschlüsselungstechnologien zur Unterstützung von Datenschutz und Sicherheit einsetzt. **Alle Kundendaten, die vom Client zur Zoom-Cloud übermittelt werden, werden während der Übertragung mithilfe einer der folgenden Methoden verschlüsselt.**

## TLS 1.2

HTTPS ist die bevorzugte Kommunikationsmethode für Verbindungen zwischen dem Zoom-Client und der Zoom-Cloud. Diese Verbindungen setzen die Transportverschlüsselung TLS 1.2 und PKI-Zertifikate, die von einer vertrauenswürdigen kommerziellen Zertifikatsinstanz ausgestellt werden, ein. Zu den weit verbreiteten Anwendungsfällen gehören das Anmelden auf dem Client, Planung eines Meetings, Chatten, Polling, Dateifreigabe und F&A während eines Meetings. TLS 1.2 dient ebenfalls als Sicherungsprotokoll für andere Kommunikationsdatenströme wie Meeting-Echtzeitinhalte.

## AES

Bei Anwendungsfällen wie Meeting-Echtzeitinhalten (Video, Sprache und Inhaltsfreigabe), in denen Daten über das User Datagram Protocol (UDP) übermittelt werden, verwenden wir AES-256 im ECB-Modus, um diese komprimierten Datenströme zu verschlüsseln. Wir haben vor, in Kürze auf AES-256 GCM umzusteigen. Darüber hinaus bleiben nach AES verschlüsselte Video-, Sprach- und Inhaltsfreigabedaten, wenn Sie nach der Verschlüsselung über den Meetingserver von Zoom laufen, weiterhin verschlüsselt, bis sie einen anderen Zoom-Client oder Zoom-Connector erreichen, der hilft, sie in ein anderes Protokoll zu übersetzen.

## SRTP

Unser Zoom Phone Produkt verwendet die Übertragungsvariante Secure Real-time Transport Protocol (SRTP), um Telefongespräche während der Übermittlung von und zu unseren Datenzentren nach AES-128-ECB zu verschlüsseln und dadurch zu schützen. Diese Funktionalität wird bald auf AES-256 GCM hochgestuft.

# Wenn ein Web Browser benutzt wird

Zoom bietet eine Weboberfläche mit reichhaltigen Funktionen, darunter eine vollständige Verwaltungskonsole, Zugriff auf Cloud-Aufzeichnungen, umfangreiche API-Endpunkte und einen webbasierten Client für Meetings. **Alle Kundendaten, die von einem Webbrowser, darunter von unserer Webseite und über unseren Webmeeting-Client, zur Zoom-Cloud übermittelt werden, werden während der Übertragung mithilfe einer der folgenden Methoden verschlüsselt.**

## TLS 1.2

Verbindungen zur Zoom Webseite verwenden Verschlüsselung mithilfe von TLS 1.2 und PKI-Zertifikate, die von einer vertrauenswürdigen kommerziellen Zertifikatsinstanz ausgestellt werden. Durch dieses Portal haben Benutzer Zugriff auf eine Reihe von Funktionen, die mit ihrem Zoom-Konto verknüpft sind, sie können deren Vorgänge verwalten und sie mit anderen Systemen integrieren. Die Stärke der Verschlüsselung und bestimmter Chiffren, die für die Verbindungen zu der Webseite verwendet werden, hängt vom Browser, mit dem die Seite aufgerufen wird, ab und davon, welche gemeinsame Verschlüsselungsmethode ausgehandelt wird.

## AES-256

Zoom setzt für bestimmte Anwendungsfälle zusätzliche Verschlüsselung über die Verwendung von TLS hinaus ein. So werden z. B. alle Kundendaten wie Cloud-Aufzeichnungen, Chat-Verlauf und Meeting-Metadaten im Ruhezustand mithilfe von AES-256 GCM verschlüsselt und die Schlüssel werden in einem Schlüsselverwaltungssystem in der Cloud verwaltet. Wenn Benutzer mit dem Zoom Web-Client eine Verbindung zu einem Meeting herstellen und dabei Web Assembly einsetzen, sendet und empfängt Zoom Echtzeitinhalte vom Meeting (Video, Sprache, Inhaltsfreigabe) über User Datagram Protocol (UDP) verschlüsselt mithilfe von AES-256 ECB direkt vom Meetingserver.

# Wenn ein Drittparteiengerät/-dienst verwendet wird

Als offene Plattform bietet Zoom verschiedene Methoden, mit denen eine Reihe von Diensten und Geräten sich mit unserem System verbinden können. Dazu gehört Unterstützung für Anwendungsfälle wie H323/SIP-Geräte, die sich mit einem Zoom-Meeting verbinden, über beliebte Streamingdienste senden und sich über eine Standard Telefonleitung in ein Meeting einwählen (also nicht über unsere App). Da diese Integrationen Kommunikationsprotokolle verwenden müssen, die nativ von dem jeweiligen Drittparteiengerät oder -dienst unterstützt werden, bleiben die Verschlüsselungsmethoden auf diejenigen, die auf diesem Gerät möglich sind, beschränkt. **Obwohl wir die Verwendung von Verschlüsselung bei Drittparteiengeräten und -diensten empfehlen, kann es daher sein, dass Kundendaten, die über diese Geräte und Dienste übermittelt werden, während der Übertragung an und vom Zoom System nicht verschlüsselt werden. Trotzdem werden Daten, wenn sie das System von Zoom erreichen, an diesem Punkt verschlüsselt und bleiben, solange sie in unseren System unterwegs sind, die ganze Zeit verschlüsselt.** Wenn ein Drittparteiengerät Verschlüsselung unterstützt, wird aller Wahrscheinlichkeit nach mit den folgenden Methoden verschlüsselt.

### TLS 1.2

Wenn das Gerät dies unterstützt, handelt Zoom die Verbindung über TLS 1.2 aus. Zum Beispiel, wenn ein SIP-Gerät Verschlüsselung aktiviert hat, dann wird TLS für die Signalgebung verwendet.

### AES

Wenn das Gerät dies unterstützt, handelt Zoom die Verschlüsselung von Meetinginhalten wie Video, Audio und Bildschirmfreigabe mithilfe von AES auf einem SIP oder H323-Endpunkt aus.

# Schlussfolgerung

In der Welt von heute, in der Zusammenarbeit über mehrere Medien und Kommunikationsplattformen hinweg stattfindet, hat sich Zoom dem Schutz seiner Kunden verschrieben. Wenn Drittparteiengeräte in die Gemengelage eingebracht werden, bieten wir die Möglichkeit, die Verschlüsselung auf eine breite Auswahl an Integrationen außerhalb unserer Plattform auszuweiten. Innerhalb unserer Plattform stellen wir sicher, dass Kundeninhalte verschlüsselt sind.