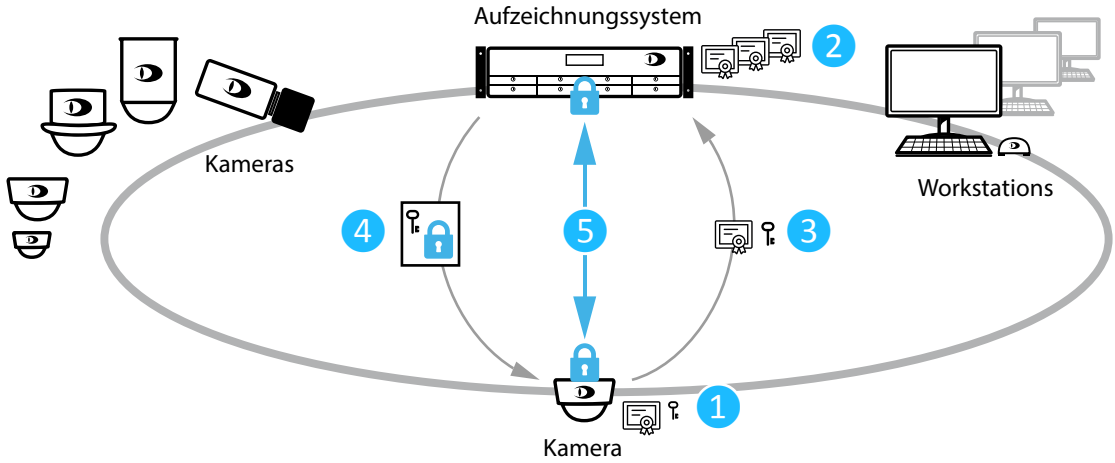
Verschlüsselte Übertragung

Absicherung des Video-Netzwerks durch verschlüsselte Übertragung (TLS 1.2 / AES 256 Bit) mit DaVids und HTTPs

Die **Kameras der Serie 5000** wurden mit einem besonderen Augenmerk auf die **Systemsicherheit** entwickelt und unterstützen die **verschlüsselte Daten- und Video-Übertragung** (TLS 1.2/AES-256) sowie die **sichere Netzwerkauthentifizierung** (IEEE 802.1X). Weitere Sicherheitsmaßnahmen umfassen die Benutzerverwaltung, den Passwortschutz, die Deaktivierung nicht benötigter oder unsicherer Ports, die regelmäßige Bereitstellung von Firmware-Updates sowie die Verhinderung der Ausführung von Fremd-Software.

Betreiber von Videoanlagen zur Absicherung von öffentlichen Plätzen, Flughäfen, Casinos oder Unternehmen sind in der Regel mit dem Problem konfrontiert, dass **Kameras am physischen Rand des Netzwerks montiert** sind. Da diese Kameras für Dritte zugänglich sind, erhöht sich das **Risiko eines ungewollten Zugriffs auf das Netzwerk**. Ein Angreifer könnte statt der Kamera ein eigenes Gerät anschließen, um Zugang zum Netzwerk zu erhalten oder den Datenverkehr auszulesen (Man-in-the-Middle-Angriff).

Neben einer sicheren Netzwerkauthentifizierung nach IEEE 802.1X kann dieses Risiko vor allem durch die **verschlüsselte Daten- und Video-Übertragung zwischen der Kamera und dem Aufzeichnungssystem** abgeschwächt werden. Dabei bietet sich der **Einsatz der Kamera-Serie 5000** an, denn alle Modelle unterstützen die **verschlüsselte Übertragung (TLS 1.2 / AES 256 Bit)** mit **DaVids und HTTPs**.



1 Kamera

Die Kamera ist mit einem individuellen Zertifikat (Ausweis) und einem öffentlichen Schlüssel (öffentliche Codeschablone) ausgestattet.

Die sichere Authentifizierung der Kamera im Netzwerk erfolgt bereits beim physikalischen Anschluss nach dem Standard IEEE 802.1X.

2 Aufzeichnungssystem

Das Aufzeichnungssystem ist mit mehreren Zertifikaten ausgestattet (Kartei). Diese erlauben den Abgleich verschiedener Kamera-Zertifikate (Ausweise). Eine Internet-Verbindung zu einem Zertifikate-Anbieter (Meldebehörde) ist nicht erforderlich.

Alle Zertifikate sind mehrstufig mit HASH-Codes signiert. Eine erfolgreiche Fälschung durch einen Angreifer kann ausgeschlossen werden.

3 Prüfung

Wenn der Video-Stream der Kamera aufgezeichnet werden soll, fordert das Aufzeichnungssystem zunächst das Zertifikat und den öffentlichen Schlüssel der Kamera an.

Durch einen Abgleich des Kamera-Zertifikats mit den hinterlegten Zertifikaten stellt das Aufzeichnungssystem die Identität der Kamera fest.

Ein Angreifer mit einer Berechtigung zum Netzwerkzugriff, aber ohne gültigem Zertifikat wird hier abgewiesen.

4 Vorbereitung

Wenn das Aufzeichnungssystem die Gültigkeit des Zertifikats (Ausweis) und die Eignung des Inhabers (Kamera) zur Aufzeichnung festgestellt hat, wird die Verschlüsselung vorbereitet.

Das Aufzeichnungssystem erzeugt einen geheimen Schlüssel (geheime Codeschablone). Dieser wird mit dem öffentlichen Schlüssel verschlüsselt und an die Kamera übertragen.

Nur die Kamera verfügt über ein Gegenstück zu ihrem öffentlichen Schlüssel, das nicht versendet wird. Nur dieser private Schlüssel erlaubt die Entschlüsselung der mit dem öffentlichen Schlüssel geschützen Daten.

5 Verschlüsselung

Die Kamera entschlüsselt den geheimen Schlüssel mit dem Gegenstück ihres öffentlichen Schlüssels, dem privaten Schlüssel.

Ab diesem Zeitpunkt wird der Video-Stream (und alle weiteren Daten) vor der Übertragung mit dem geheimen Schlüssel verschlüsselt. Das Aufzeichnungssystem entschlüsselt den Video-Stream und speichert die Bilder in Echtzeit.

Nur die Kamera und das Aufzeichnungssystem verfügen über den geheimen Schlüssel. Kein anderer Netzwerkteilnehmer (zweites Aufzeichnungssystem, Workstation, etc.) kann den Video-Stream der Kamera entschlüsseln.

Dieses Handout beschreibt die verschlüsselte Übertragung mit TLS/AES stark vereinfacht. Detaillierte technische Informationen finden Sie in https://de.wikipedia.org/wiki/Transport_Layer_Security.