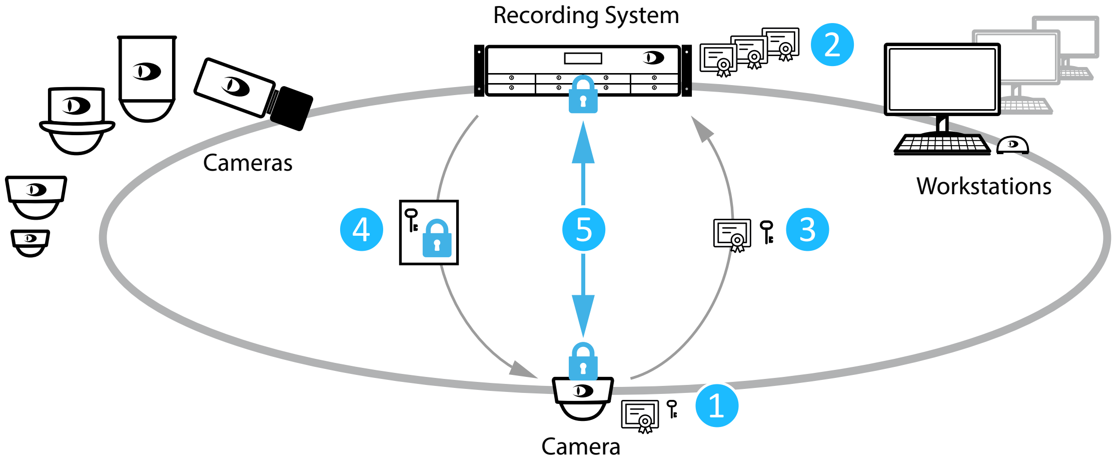
Encrypted Transmission

Protection of the video network by encrypted transmission (TLS 1.2 / AES 256 bit) with DaVids and HTTPs

Designed with a special focus on **system security,** the **5000 series cameras** support **encrypted data and video transmission** (TLS/AES-256) along with **secure network authentication** (IEEE 802.1X). Other security measures include user management, password protection, deactivation of unneeded or insecure ports, regular provision of firmware updates as well as the prevention of third-party software execution.

Operators of video systems for the security of public places, airports, casinos or businesses are usually confronted with the problem that **cameras are mounted on the physical edge of the network**. Since these cameras are accessible to third parties, the **risk of unwanted access to the network** increases. An attacker could connect his own device instead of the camera to gain access to the network or read out the data traffic (man-in-the-middle attack).

In addition to authentication in accordance with IEEE 802.1X, this risk can be mitigated by **encrypted data and video transmission between the camera and the recording system**. The **use of the 5000 series cameras** is recommended, as all models support **encrypted transmission (TLS 1.2 / AES 256 bit)** with **DaVids and HTTPs**.



1 Camera

The camera is equipped with an individual certificate (ID card) and a public key (public encryption template).

ⓘ The secure authentication of the camera in the network is already carried out during the physical connection according to the standard IEEE 802.1X.

2 Recording System

The recording system is equipped with several certificates (register). These allow the comparison of various camera certificates (ID cards). An Internet connection to a certificate provider (regulatory authority) is not required.

ⓘ All certificates are multilevel signed with HASH codes. A successful falsification by an attacker can be ruled out.

3 Check

If the camera's video stream is to be recorded, the recording system first requests the camera's certificate and public key.

By comparing the camera certificate with the stored certificates, the recording system determines the identity of the camera.

ⓘ An attacker with permission to access the network but without a valid certificate is rejected here.

4 Preparation

Once the recording system has verified the validity of the certificate (ID card) and the suitability of the holder (camera) for recording, encryption is prepared.

The recording system generates a secret key (secret encryption template). This is encrypted with the public key and transmitted to the camera.

ⓘ Only the camera has a counterpart to its public key that is not sent. Only this private key allows decryption of data protected with the public key.

5 Encryption

The camera decrypts the secret key with the counterpart of its public key, the private key.

From this point on, the video stream (and all other data) is encrypted with the secret key before transmission. The recording system decrypts the video stream and saves the images in real time.

ⓘ Only the camera and recording system have the secret key. No other network device (second recording system, workstation, etc.) can decrypt the video stream of the camera.

ⓘ This handout describes the encrypted transmission with TLS/AES in a simplified way. Detailed technical information can be found at https://en.wikipedia.org/wiki/Transport_Layer_Security.