WHITE PAPER

Security in Axis body worn solution

February 2024

Summary

Despite being based on an open platform, the Axis body worn system enjoys a very high level of system security.

To ensure security in case of camera loss, the camera is based on a minimized platform with no unnecessary software components. More features are instead placed in the system controller, which is usually less exposed to physical threats. Furthermore, the camera's internal storage is AES-256 encrypted to prohibit unauthorized access to data. Communication based on IPv6 and certificates ensure that the camera will offload data only to the specific system controller or system it belongs to.

When data is offloaded from the camera to the system controller, an HTTPS encrypted network connection is used. The data is only briefly stored in the system controller's AES-256 encrypted storage device, before being further transferred, using another HTTPS encrypted connection, to the content destination.

The security and integrity of the system controller is further strengthened by a FIPS 140-2 compliant TPM (trusted platform module). Other features, which the body worn system shares with many other Axis devices, are signed firmware, secure boot, and signed video.

When footage is live streamed through AXIS Body Worn Live, the data is encrypted at rest, in transport, and in the viewer's web browser. It is also end-to-end encrypted with the protocol XChaCha20-Poly1305. Furthermore, the administrator controls who can view the live stream, right down to the specific computer, web browser, and user credentials.

Table of Contents

1 Acronyms and terminology 4
2 Introduction 4
3 Security in case of camera loss 4
4 Security in data transfer 4
5 Other security features 5
6 Security with AXIS Body Worn Live 5

1 Acronyms and terminology

BWC. Body worn camera

VMS. Video management system

EMS. Evidence management system

Content destination. A location which stores recordings and data from, for example, body worn cameras. Examples of content destinations include video management systems, evidence management systems, and media servers.

2 Introduction

The Axis body worn system is based on an open platform, which makes it easy to integrate with external systems for video management and evidence management. Nevertheless, it enjoys a very high level of system security because this was the main focus in every step in the implementation of the system.

This white paper outlines the data flow between the components in the Axis body worn system. We especially describe the measures taken to secure the system and its data, all the way from a BWC recording to the content destination. The different storage media are also highlighted including additional security considerations.

3 Security in case of camera loss

Through its everyday use, the body worn camera (BWC) is physically exposed to the risks of theft and vandalism. Several system design features were employed in order to mitigate the effects of such threats so that system and data security is maintained even if a camera goes missing.

One example is that the BWC is based on a minimized software platform compared to that of other Axis cameras, and all unnecessary software components have been removed. The camera and the system controller have no VAPIX support, nor any support for protocols such as FTP, SSH, or SNMP. Furthermore, the camera has no server functionality. Integration with other systems, such as VMS and EMS, is instead handled by the system controller, which is usually less exposed to physical threats than the cameras are.

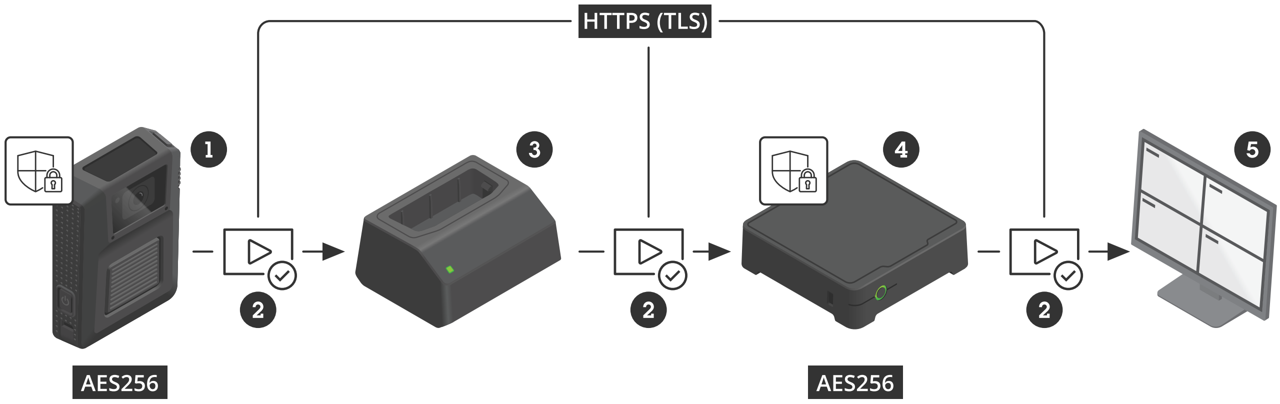
The BWC's internal storage is encrypted using AES-256 to prohibit unauthorized access to data in case of camera loss.

The camera will offload data only to the one specific system controller or system it belongs to. This is because the BWC and the system controller communicate with IPv6 and using certificates. The certificates are automatically renewed to match the latest from the system controller every time the camera is docked.

Should a camera be undocked and away from the system for more than four weeks, there is a grace period when the system controller accepts older certificates for eight weeks. Should a camera be away longer than that, it needs to be manually accepted into the system again, using the master key passphrase. This is to ensure that a camera that has been lost or away for a long time cannot be unnoticeably added again, as this might pose a security risk.

4 Security in data transfer

In typical use, the BWC is docked after a full shift, containing videos and metadata. All the data is offloaded through the docking station to the system controller using a network connection encrypted with HTTPS (HTTP with TLS). The data is stored in the system controller only briefly, on its SSD storage device which is encrypted using AES-256. The system controller then transfers the data, using HTTPS, to the content destination.



Secure data transfer and storage, from the BWC (1) to the content destination (5).

1 *BWC with Axis Edge Vault*
2 *Signed video (cybersecurity feature)*
3 *Docking station*
4 *System controller with Axis Edge Vault*
5 *Content destination*

There is also support for using an encryption key from the content destination to encrypt the data in the BWC and system controller, if the content destination provides a public encryption key. In that case the data will have an extra layer of encryption when being sent to the content destination.

5 Other security features

The security and integrity of the system controller is further strengthened by a FIPS 140-2 compliant TPM (trusted platform module).

Both the BWC and the system controller are equipped with Axis Edge Vault, a hardware-based cybersecurity platform that protects all data on the devices and enables several security features. For example, the file system is encrypted and the key is protected by Axis Edge Vault. *Secure boot* ensures that the devices can boot only with authorized firmware. *Signed firmware* makes them reject firmware upgrades if the firmware integrity is compromised. *Signed video* creates an extra layer of protection by adding a cryptographic checksum into the video stream. This allows the video to be reliably traced back to the unique Axis camera where it was produced, verifying that the footage has not been tampered with.

See *www.axis.com/developer-community/signed-video* for more details about signed video, or *www.axis.com/solutions/built-in-cybersecurity-features* for more details about Axis cybersecurity features.

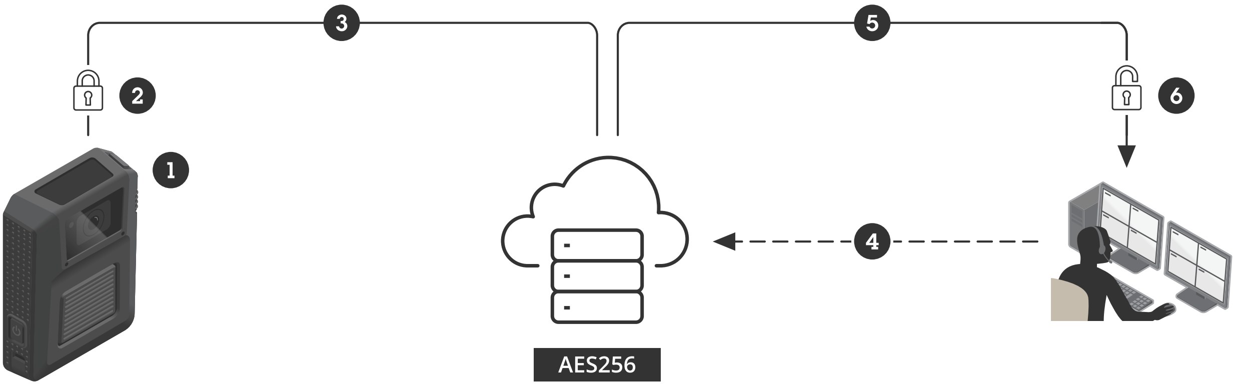
The only way for the camera user to view recorded video in the field is via the application AXIS Body Worn Assistant. If the application is enabled, the BWC streams video directly to the application, but no video material is stored for later access in the cache or memory of the device running the application. There is also an overlay in the video stream to deter the use of secondary recording devices to capture the video. If this is still done, the video clip can be tracked to the BWC user via the overlay. The USB-C compatible connector of the BWC cannot be used in any way to view, delete, or offload the video.

6 Security with AXIS Body Worn Live

AXIS Body Worn Live is an application that allows access to live data from Axis body worn cameras. By providing users with a live stream of video, audio, and other data, such as location coordinates, AXIS Body Worn Live enables unparalleled situational awareness of an ongoing incident. It is initially provided as a cloud-based service.

With AXIS Body Worn Live, the data is encrypted not only at rest (in storage) and in transit, but also fully end-to-end encrypted between the camera and the viewer's web browser.

All data and files hosted in AXIS Body Worn Live are encrypted using AES-256 at rest. All communication channels are secured using HTTPS with TLS, employing certificates signed by trusted certificate authorities. AXIS Body Worn Live also adds another layer of true end-to-end encryption with the protocol XChaCha20-Poly1305.



Secure live streaming with end-to-end encryption in AXIS Body Worn Live

1 *BWC collects live video and other data.*
2 *Data is encrypted in the BWC.*
3 *Data is transmitted from BWC to AXIS Body Worn Live.*
4 *The viewer requests data from AXIS Body Worn Live.*
5 *Data is streamed from AXIS Body Worn Live to the viewer.*
6 *Data is decrypted in the viewer's web browser.*

The administrator of the body worn camera system is in full control of who can view the live stream. The data is encrypted in such a way that only the viewers approved by the administrator can decrypt and view the video, and the administrator can also revoke access. The viewer must have the right computer, the right web browser, and the right user credentials. No one else, not even Axis, can access the live stream. Axis has no access to user-created end to end encryption keys.

T10155258/EN/M8.4/2402

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.