WHITE PAPER

Axis body worn cameras

System security

June 2020

Table of Contents

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 AES256 to prohibit unauthorized access to data in case of camera loss.

The camera will only offload data 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 can't 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 AES256. The system controller then transfers the data, using HTTPS, to the content destination.

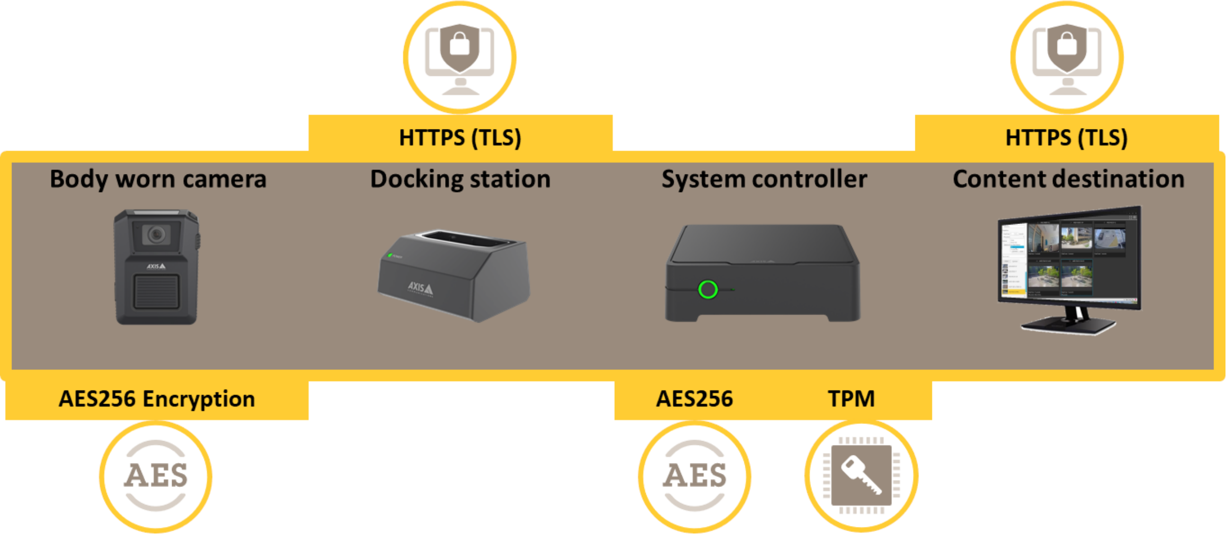

Figure 1. Secure data storage and data transfer from the BWC to the content destination.

There is also support for using an encryption key from the content destination to encrypt the data in the BWC and system controller, should the content destination choose to provide 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) as well as the secure boot feature which ensures that the device can boot only with authorized firmware. Furthermore, both the system controller and BWC have the signed firmware feature which makes them reject firmware upgrades if the firmware integrity is compromised.

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 from using secondary recording devices to capture the video. Should that still be the case the 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.

T10155258/EN/M1.3/2006

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems.

Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website *axis.com*.

AXIS® COMMUNICATIONS