From BT-VS/MKP	Product Management		Nuremberg 06.05.2022

Release Letter

Products:	***Combined Signed Firmware for*** ***CPP7.3 UHD/HD/MP cameras*** ***CPP7 HD/MP cameras*** ***CPP6 UHD/MP cameras*** ***CPP4 HD cameras***
Version:	***7.84****.0506*

This letter contains latest information about the above mentioned firmware version.

1 General

This firmware release is a combined and signed firmware package, applicable to H.264 and H.265 products based on one of the following platforms.
It can be used to upgrade firmware on cameras of the applicable platforms running firmware version 6.51 or higher.

This combined and signed firmware supports platforms only that force a two-factor authenticated release signature and accept encrypted firmware files to help increase the overall security level.

Firmware release 7.84 is the last feature release for CPP6, CPP7 and CPP7.3 cameras. Firmware will be maintained for field and security issues.

From			Nuremberg
BT-VS/MKP	Product Management		06.05.2022

This firmware supports:

- CPP7.3 HD and UHD cameras
  - upgrade from FW 6.51 or newer to latest FW 7.84
- CPP7 HD cameras
  - upgrade from FW 6.51 or newer to latest FW 7.84
- CPP6 HD and UHD cameras
  - upgrade from FW 6.51 or newer to latest FW 7.84
- CPP4 HD and MP cameras
  - upgrade from FW 6.51 or newer to latest FW 7.10

The combined firmware package includes the following build versions:

- CPP7.3 FW 7.84.0023
- CPP7 H.264 7.84.0023
- CPP6E H.264 7.84.0023
- CPP6 H.264 7.84.0023
- CPP4 H.264 7.10.0096

For detailed description please refer to the separate release letters.

From			Nuremberg
BT-VS/MKP	Product Management		06.05.2022

2 Important notes

2.1 End of Feature for CPP6, CPP7 and CPP7.3 – Maintenance mode started

With release of FW 7.84, feature implementation for the platforms CPP6, CPP7 and CPP7.3 ends, and the firmware development will switch over into maintenance mode. The firmware branch 7.8 for these platforms is now treated as a **long-term supported firmware (LTSFW)**, with its code base frozen to allow bug fixing and applying security fixes where necessary.

2.2 End of Feature for CPP4 – Maintenance mode started

With release of FW 7.10, feature implementation for the CPP4 platform ends, and the firmware development will switch over into maintenance mode. The firmware branch for CPP4 is now treated as a **long-term supported firmware (LTSFW)**, with its code base frozen to allow bug fixing and applying security fixes where necessary.

2.3 Two-factor authenticated firmware signature

The security of the signature of the firmware file has been strengthened by using a two-factor authentication process for signing the final firmware file. This new process has been prepared for with firmware 6.50 and comes into effect with succeeding versions, from firmware 6.51 onwards.

The new signature protects from non-released versions being installed in production systems. As a result, pre-release (beta) versions, required sometimes in projects, need to have a special license installed prior to the firmware update. Requests for pre-release versions need to be handled via tech support tickets in order to allow tracking and require a concession signed by the customer.

Note:

This combined firmware file is not applicable to devices running firmware older than FW 6.51 due to the two-factor authenticated release signature and firmware file encryption.
For such devices apply the unsigned combined firmware file or the platform-specific firmware up to firmware 6.51 before using this combined and signed firmware.

2.4 Firmware file encryption

This combined and signed firmware includes signed and encrypted firmware files only. Thus, only platforms that support firmware file decryption are applicable to this combined and signed firmware.

2.5 Secure Element ("TPM")

All devices incorporate a secure microcontroller, which we call our Secure Element.
"A Secure Element is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities."[1] In this specific case the requirements are defined in the Trusted Platform Module library specification defined by the Trusted Computing Group (TCG). As the Secure Element supports the main functionalities specified by TCG, the ones needed for an IoT device, it is often referred to as a "TPM".
Due to security reasons, the firmware or functionality of the secure crypto-microcontroller cannot be altered in the field.
Thus, not all new security features become available on devices with older secure crypto-microcontroller hardware or firmware revisions.

2.6 Open Source Software

Bosch Security Systems is advocate of integrating open source software into its products. The use of open source software is noted in the *Service* menu on the *System Overview* page of every camera's web interface. For general information regarding open source software in Bosch Security Systems, please visit http://www.boschsecurity.com/oss .

[1] https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf, page 1

3 Applicable products

CPP7.3

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 5000i (IR)
- AUTODOME IP starlight 5100i (IR)
- AUTODOME IP starlight 7000i
- DINION IP 3000i
- DINION IP bullet 4000i
- DINION IP bullet 5000
- DINION IP bullet 5000i
- DINION IP bullet 6000i
- FLEXIDOME IP 3000i
- FLEXIDOME IP 4000i
- FLEXIDOME IP 5000i
- FLEXIDOME IP indoor 8000i (– X series)
- FLEXIDOME IP starlight 5000i (IR)
- FLEXIDOME IP starlight 8000i
- FLEXIDOME IP starlight 8000i (– X series)
- MIC IP starlight 7000i
- MIC IP starlight 7100i
- MIC IP ultra 7100i
- MIC IP fusion 9000i

CPP7

- DINION IP starlight 6000
- DINION IP starlight 7000
- DINION IP thermal 8000
- FLEXIDOME IP starlight 6000
- FLEXIDOME IP starlight 7000
- DINION IP thermal 9000 RM

From			Nuremberg
BT-VS/MKP	Product Management		06.05.2022

CPP6

- DINION IP starlight 8000 12MP
- DINION IP ultra 8000 12MP
- DINION IP ultra 8000 12MP with C/CS mount telephoto lens
- FLEXIDOME IP panoramic 6000 12MP 180
- FLEXIDOME IP panoramic 6000 12MP 360
- FLEXIDOME IP panoramic 6000 12MP 180 IVA
- FLEXIDOME IP panoramic 6000 12MP 360 IVA
- FLEXIDOME IP panoramic 7000 12MP 180
- FLEXIDOME IP panoramic 7000 12MP 360
- FLEXIDOME IP panoramic 7000 12MP 180 IVA
- FLEXIDOME IP panoramic 7000 12MP 360 IVA

From			Nuremberg
BT-VS/MKP	Product Management		06.05.2022

CPP4

- AUTODOME IP 4000 HD
- AUTODOME IP 5000 HD
- AUTODOME IP 5000 IR
- AUTODOME 7000 series
- DINION HD 1080p
- DINION HD 1080p HDR
- DINION HD 720p
- DINION imager 9000 HD
- DINION IP bullet 4000
- DINION IP bullet 5000
- DINION IP 4000 HD
- DINION IP 5000 HD
- DINION IP 5000 MP
- DINION IP starlight 7000 HD
- FLEXIDOME corner 9000 MP
- FLEXIDOME HD 1080p
- FLEXIDOME HD 1080p HDR
- FLEXIDOME HD 720p
- Vandal-proof FLEXIDOME HD 1080p
- Vandal-proof FLEXIDOME HD 1080p HDR
- Vandal-proof FLEXIDOME HD 720p
- FLEXIDOME IP micro 2000 HD
- FLEXIDOME IP micro 2000 IP
- FLEXIDOME IP indoor 4000 HD
- FLEXIDOME IP indoor 4000 IR
- FLEXIDOME IP outdoor 4000 HD
- FLEXIDOME IP outdoor 4000 IR
- FLEXIDOME IP indoor 5000 HD
- FLEXIDOME IP indoor 5000 MP
- FLEXIDOME IP micro 5000 HD
- FLEXIDOME IP micro 5000 MP
- FLEXIDOME IP outdoor 5000 HD
- FLEXIDOME IP outdoor 5000 MP
- FLEXIDOME IP panoramic 5000
- IP bullet 4000 HD
- IP bullet 5000 HD
- IP micro 2000
- IP micro 2000 HD
- MIC IP dynamic 7000
- MIC IP starlight 7000
- TINYON IP 2000 family

From			Nuremberg
BT-VS/ETP-MKP1	Product Management		06.05.2022

4 New Features for CPP7.3

- Bandwidth throttling has been added to allow the camera being installed on networks with limited throughput capacity. The available bandwidth can be configured as kbps values in the Ethernet section of the Network Access menu. The camera will then limit its data generation on the network to this maximum Ethernet transmission value to avoid bursts in the network traffic. The Ethernet input on the camera is not limited.
- The Network Access menu has been separated for IPv4 and IPv6 addresses. IPv4 and IPv6 can now separately be configured and activated.
- IP filter entries have been extended to allow up to 20 IP addresses or ranges.
- For certificate-based network authentication, and in case of an unsubstantiated time base, the camera may assume its time from the overlapping validity periods in the EAP-TLS certificates, if this feature is enabled via the camera's settings.
  With valid certificates, this will allow the camera to connect to the network even in case of an invalid system time due to e. g. a longer power loss.

5 Changes for CPP7.3

- An issue is fixed where insufficient memory allocation caused sporadic unresponsiveness of a camera's web user interface.
- An issue is fixed where a wrong color was applied to alarm-triggered bounding boxes when using Camera Trainer.
- An issue is fixed where black video was randomly and/or temporarily shown on MIC IP ultra after firmware upgrade.
- An issue is fixed where metadata from optical and thermal sensors were misaligned for video fusion in MIC 9000i.

6 New Features for CPP6 and CPP7

- Bandwidth throttling has been added to allow the camera being installed on networks with limited throughput capacity. The available bandwidth can be configured as kbps values in the Ethernet section of the Network Access menu. The camera will then limit its data generation on the network to this maximum Ethernet transmission value to avoid bursts in the network traffic. The Ethernet input on the camera is not limited.
- The Network Access menu has been separated for IPv4 and IPv6 addresses. IPv4 and IPv6 can now separately be configured and activated.
- IP filter entries have been extended to allow up to 20 IP addresses or ranges.
- For certificate-based network authentication, and in case of an unsubstantiated time base, the camera may assume its time from the overlapping validity periods in the EAP-TLS certificates, if this feature is enabled via the camera's settings.
  With valid certificates, this will allow the camera to connect to the network even in case of an invalid system time due to e. g. a longer power loss.

7 Changes for CPP6 and CPP7

- An issue is fixed where insufficient memory allocation caused sporadic unresponsiveness of a camera's web user interface.
- An issue is fixed where a wrong color was applied to alarm-triggered bounding boxes when using Camera Trainer.

Please check the platform-specific release notes of FW 7.84.0023 for completeness and details.

From			Nuremberg
BT-VS/ETP-MKP1	Product Management		06.05.2022

8 Changes for CPP4

- An issue is fixed where MSS and MTU settings may have come out of sync. During a write to the MTU size, the MSS is now checked and, if fragmentation would occur, would implicitly be adjusted to a value of MTU-40, before the MTU is reduced.

Please check the platform-specific release notes of FW 7.10.0096 for completeness and details.

9 Restrictions; Known Issues

- This combined firmware file is not applicable to devices running firmware older than FW 6.51 due to the two-factor authenticated release signature and firmware file encryption.
- Video authentication using SHA hashing mechanisms are not functional if no self-signed certificate has been created yet. Opening an HTTPS connection once is prerequisite.
- Cameras with security coprocessor version 3 with an externally applied certificate will fail HTTPS connections requesting SHA256. The restriction applies to all functions using the private key from the certificate, including
  - EAP-TLS with client authentication
  - TLS-Time with client authentication
  - TLS-Syslog with client authentication

  With self-signed certificate, HTTPS is fully functional.
- Creating 2048 bit keys for self-signed certificates may take more than 20 seconds, extending the initial boot cycle, which may occasionally cause a timeout on the very first HTTPS connection to a camera. The next connection attempt typically is successful.
- Software sealing does not cover all static parameters of image pre-processing and moving camera control.
- If software sealing is active and SNMP is disabled in Network -> Network Services, no SNMP trap will be sent out on seal break due to the disabled service. The seal break itself is logged.
- Creating 2048 bit keys for self-signed certificates may take more than 20 seconds, extending the initial boot cycle, which may occasionally cause a timeout on the very first HTTPS connection to a camera. The next connection attempt typically is successful.
- Software sealing does not cover all static parameters of image pre-processing and moving camera control.
- If software sealing is active and SNMP is disabled in Network -> Network Services, no SNMP trap will be sent out on seal break due to the disabled service. The seal break itself is logged.
- This combined firmware file is not applicable to devices running firmware higher than FW 6.50 due to the 2-factor release signature.
- AVIOTEC firmware is not included in this combined firmware file.

Please check the respective release letter of a camera or encoder for further device-specific restrictions.

10 System Requirements

Possible clients for configuration purposes:

- Configuration Manager 7.50 or newer
- Web Browsers:
  - Google Chrome
  - Microsoft Internet Explorer 11 or higher
  - Microsoft Edge (Chromium based)
  - Mozilla Firefox

Possible clients for operation purposes:

- Bosch Video Security App 1.2 or higher
- Bosch Video Security Client 2.0 or higher
- Web Browsers:
  - Google Chrome
  - Microsoft Internet Explorer 11 or higher
  - Microsoft Edge (Chromium based)
  - Mozilla Firefox
- DirectX 11
- MPEG-ActiveX 6.34 or newer (for IE only)