SeeTec
An OnSSI Company

Data protection and data integrity in SeeTec Cayuga

Version	Date
1.1	07.05.2018

Content

SeeTec GmbH has integrated several security features in its SeeTec Cayuga software to ensure data protection, data integrity and data confidentiality according to the General Data Protection Regulation (GDPR).

1. Encrypted communication between SeeTec Cayuga Server and SeeTec Cayuga Client

- The communication between the Client and Server modules is encrypted.
  SeeTec uses a 128-bit AES encryption key.
- The password is always transmitted from the SeeTec Cayuga Client to the SeeTec Cayuga Server as “salted SHA-512 hash”.
  SSL certificates are used to protect the software against man-in-the-middle attacks.

2. Encrypted communication between the camera and the SeeTec Cayuga Server

- The transmission of video and audio from the camera to the SeeTec Server can be encrypted using HTTPS, depending on if the camera supports it.
  TLS 1.2 can be used for supported camera models, i.e. if supported by the camera and implemented for this camera model by SeeTec (ref. our supported devices data base).

3. Display images / storing images / exporting images

- Data in the SeeTec MultimediaDatabase (MDB) is stored encrypted in a proprietary format. We assume that physical access to the storage server has been restricted by administrative actions.
- The retention times can be set individually for each camera and separately for standard- and alarm-recording.
- Export from the MDB is 3DES (Triple DES) encrypted. Any alteration on the exported data will result in the password not working and therefore confirms the export is valid. The protection of the raw data prevents manipulation and ensures the authenticity of the data.
- Time-based / event-based recording is possible (e.g. recording only outside of working hours and/or during an event).
- Cameras can be activated or deactivated based on an event.
- Masking of the camera image.
  - Sensitive image areas can be masked by a freely definable area.
  - Dynamic masking for moving objects is supported.
  - Both methods are available in surveillance mode and archive mode.
  - All masks are subject to user authorization.

4. User rights management / user access

- For each user the following authorizations can be set individually:
  - **Surveillance camera**: The user can see a camera and its live images in surveillance mode.
  - **Camera archive**: The user can use cameras in archive mode.
  - **Delete recordings**: The user can delete recordings in archive mode.
  - **Overwrite protection**: The user can apply overwrite protection to recordings in archive mode or remove overwrite protection from them.
  - **Camera PTZ**: The user can use the PTZ camera except for preset camera positions.
  - **Camera lock**: The user can lock the position of the PTZ camera.
  - **Use camera position**: The user can use the set camera positions.
  - **Create camera positions**: The user can create camera positions or delete positions that have been predefined.
  - **Export camera**: The user can save image data in the SeeTec specific format in archive mode.
  - **Export camera (AVI)**: The user can save image data as an AVI file in archive mode.
  - **Privacy masking**: The user can deactivate privacy masking.
  - **MPEG audio**: The user can use audio transmission.
  - **Map**: The user can use the corresponding map.
  - **Layer**: The user can display defined layers.
  - **Button**: The user can use buttons.
  - **Report mode**: The user can view the report mode.
  - **Edit report templates**: The user can create and edit report queries in report mode and save them as templates.
  - **Server extensions**: The user can use server extensions, e.g. license plate recognition.
  - **Count analysis**: The user can use the count analysis from the “View” menu.
  - **Use license plate group**: The user can use license plate groups.
  - **Change license plate group**: The user can change license plate groups.
  - **Access Control**: The user can use the access control.
  - **Access Control Data Editor**: The user can use the access control data editor from the “View” menu.

- Optional: for every user a 2nd password can be set (“dual control principle”).
- Optional: a user can be forced to change his/her password on a regular basis.
- Secure password: If the option “User must use a secure password” is activated, the password must consist of at least eight characters and contain at least one digit, one upper-case letter and one lower-case letter.
- There is a time-limited login lock after three unsuccessful login attempts (brute-force attack protection).
- Tiered user and group rights management.
- Tiered rights management for branch administrators.
- There is no backdoor in the SeeTec systems to restore a lost administrator password.
- Time-based access to live and archive images possible (e.g. access only outside of working hours).
- Microsoft Active Directory support.

5. Report mode / logging

In report mode, the following logged event types can be displayed, including date and time:

- User login.
- Mode change (surveillance-, archive, report- and configuration-mode).
- Access of archived images including camera name and date/time.
- Export of archived images including camera name and date/time.
- Camera usage.
- Guard tours.
- Actions (triggered by buttons).
- Start of alarm scenarios including user actions if required.
- Configuration changes of camera parameters.
- SeeTec Services information.
- Information about storing audio- and video-data.

All events are stored in the SeeTec management database and deleted according to the settings made by the contractor or operator of the system.
Accessing the events requires a specific user right.

6. Reference image comparison

A reference image comparison can be conducted manually or automatically. The live camera image is compared to a predefined reference image of the same camera view to ensure that the camera was view has not been changed.

7. UVV Kassen and Fiducia certification

Usage of the SeeTec Cayuga software for video surveillance in finance institutions and for ATMs has been certified according to standards put forward by the UVV Kassen and Fiducia (two German institutions that have established standards and best practice recommendations for the financial sector).

8. GDPR: Processing and transfer of personal data

Generally, audio- and video-data can be processed. However, by default, audio recording is disabled. Whether the processed data are personal data according to the General Data Protection Regulation (GDPR) mainly depends on the identifiability of the recorded person.
Audio- and video-data can be transmitted to 3rd party applications using several SeeTec interfaces (SDK, SGS; SAI).
Parts of the SeeTec Software can be included in 3rd party systems do display video- and audio-data.

9. GDPR: storing personal data / logging

- Audio- and video-data are stored/deleted according to the settings made by the contractor or operator of the system.
- User data (SeeTec username and date/time of the login) are stored in the client log file (`client.log`; Location: `C:\Users\[Windows User]\AppData\Local\SeeTec\log`) and in the log file of the core service (`core.log`; Location: `C:\Program Files\SeeTec\log`).
- Log files will be stored/overwritten according to the settings made by the contractor or operator of the system.
- User interactions (see chapter 5 Report mode / logging) are stored in the SeeTec management database and deleted after a pre-defined time range. Accessing this data requires a specific user right.
- User data (SeeTec username and password) can be saved in the client login dialogue. The user data will be stored encrypted in the file `client.conf.xml` (Location: `C:\Users\[Windows User]\AppData\Local\SeeTec\`).
- For sending system or alarm notification emails the respective personal email-addresses will be entered and saved by a SeeTec administrator in Configuration mode-> System -> Email Manager.

10. SeeTec Software Development Kit (SDK)

Applications which have incorporated the SeeTec SDK act like a SeeTec Cayuga client regarding data protection and data integrity (see chapter 1 Encrypted communication between SeeTec Cayuga Server and SeeTec Cayuga Client).
The same data are requested and stored. For the login a valid user account is needed.
For the utilization and handling of personal data outside the SDK, please refer to the manufacturer of the 3rd party application.

11. SeeTec Gateway Service (SGS), SeeTec Transcoding Service (STS)

Applications using the SGS act like a SeeTec Cayuga client regarding data protection and data integrity (see chapter 1 Encrypted communication between SeeTec Cayuga Server and SeeTec Cayuga Client).
The same data are requested and stored. For the login a valid user account is needed.
For the utilization and handling of personal data outside the SGS, please refer to the manufacturer of the 3rd party application.
Data transmission between the application and the SGS is encrypted using HTTPS.
Transcoded video streams by the STS will be delivered over RTSP and are not encrypted.
Audio data cannot be delivered via the SGS.

12. SeeTec WebClient, SeeTec MobileClient

SeeTec WebClients and MobileClients are using the Gateway Service and the Transcoding Service (See previous chapter SeeTec Gateway Service (SGS), SeeTec Transcoding Service (STS)).

13. SeeTec Access Control Interface (SACI)

Configuration and access data will be requested from the respective manufacturer plugin and stored in SeeTec Cayuga. This data will also be requested and displayed by the SeeTec Client.
Whether this data is personal data depends on the respective manufacturer plugin but is highly likely in the case of an access control.
The encryption between the SACI and the external system depends on the external interface.

14. SeeTec Analytics Interface (SAI)

Video data can be sent to the respective manufacturer plugin. Configuration and access data will be requested from the respective manufacturer plugin and stored in SeeTec Cayuga. This data will also be requested and displayed by the SeeTec Cayuga Client.
Whether this data is personal data depends on the respective manufacturer plugin but is unlikely in the case of an analytics software.

15. SeeTec Video Analysis (VA)

The VA module analyzes whether the video data includes people, vehicles, or objects that move in a certain direction or within a defined range. The analysis results (meta data) are stored together with the image data.
The transmission of the video data to the analytics module as well as the transmission of the meta data to the SeeTec Cayuga Server is encrypted using TLS 1.2.
For the configuration of the VA module (creating rules), video data will be sent to the SeeTec Analytics Server 3D Configuration Tool. This connection is also encrypted using TLS 1.2.

16. SeeTec license plate recognition (LPR)

Video data which includes license plates will be analyzed in the LPR mode.
The results will be stored in SeeTec Cayuga. The results will also be requested and displayed by the SeeTec Cayuga Client.
It is possible to add user-defined master data to a license plate. The master data then may include personal data like owner of the vehicle and/or driver.
This data can also be requested via the SGS interface.

17. Siemens SiPass Integration

Configuration and access data will be requested from the respective manufacturer plugin and stored in SeeTec Cayuga. This data will also be requested and displayed by the SeeTec Cayuga Client.
Whether this data is personal data depends on the SiPass installation but is highly likely in the case of an access control software.
It is possible to add user-defined master data (which may include personal data) to an access control card.

SeeTec GmbH
Werner-von-Siemens-Str. 2-6
76646 Bruchsal
Germany
Phone: +49 (0) 7251 9290-0
Fax: +49 (0) 7251 9290-815
E-mail: info@seetec.de
Internet: https://www.seetec-video.com