



Short Public Report

1. Name and version of the IT product:

“vimacc 2.2 – Video Management Software”

2. Manufacturer or vendor of the IT product:

Company Name:

Accellence Technologies GmbH

Address:

Garbsener Landstr. 10, 30419 Hannover, Germany

Contact Person:

Mike Plötz

3. Time frame of evaluation:

February 8th 2016 – February 8th 2017

4. EuroPriSe Experts who evaluated the IT product:

Name of the Legal Expert:

Stephan Hansen-Oest

Address of the Legal Expert:

Im Tal 10a, 24939 Flensburg, Germany

Name of the Technical Expert:

Andreas Bethke

Address of the Technical Expert:

Papenbergallee 34, 25548 Kellinghusen, Germany

5. Certification Body:

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

eMail: contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

„vimacc“ is a platform independent software for professional video management. It runs on Windows and Linux operating systems and can be installed on dedicated hardware (“on premise”) or in virtual machines in a data center. The ToE uses encryption and a sophisticated management of access rights in order to protect video data against unauthorized access.

ToE is the software “vimacc 2.2” with all standard-components which is configured by Accellence Technologies to run under the following restrictions:

- The end-to-end-encryption is activated and cannot be deactivated by an administrator of the system.
- The whole internal communication is encrypted.
- Audio-streams are deactivated and cannot be activated.
- The integrated http-server is deactivated (not part of the ToE).
- The integrated RTSP-Server is deactivated (not part of the ToE).

- The integrated vimacc-FTP-uploader is deactivated (not part of the ToE).
- The password-policies are set as delivered and cannot be deactivated, though stronger and longer passwords can be defined and used.
- An export of streams have to be encrypted and protected by passwords with defined policies concerning the complexity.
- The vimacc Control-Interface must not set to „VIMACC_CONTROL_INTERFACE_ALL=true“, which grants full access to the system.

It is worth mentioning that customers of Accellence Technologies who make use of the ToE are not able to change the privacy relevant configuration elements listed above themselves.

7. General description of the IT product:

„vimacc“ is a professional video management software. It runs on Windows and Linux platforms. With “vimacc” a user (controller) can stream and store information from video surveillance cameras. All video material is encrypted during transfer and at rest. Video material is encrypted directly in the camera (preferred mode) or in the first software interface of vimacc. Accellence Technologies advises the users of “vimacc” that the highest level of confidentiality and integrity is achieved if they make use of cameras that allow for the installation of the “vimacc” encryption module directly on the camera and thus for real end-to-end encryption.

For decrypting video data, the user needs a hardware dongle with a private decryption key. For encryption, the manufacturer uses a hybrid solution of RSA and AES encryption.

The ToE does not provide further video analysis features. The manufacturer offers several software add-ons for the analysis of video data. However, these add-ons are not part of the ToE.

„vimacc“ comes with a comprehensive access rights and device management. The user can grant differentiated access rights on a per user basis.

8. Transnational issues:

None.

9. Tools used by the manufacturer of the IT product:

- Development Environment
 - Microsoft Visual Studio
 - SubVersion
 - Jenkins
 - BugZilla
 - QT-Framework
 - FFMPEG
 - Open-SSL
 - OpenCV

- Test Environment
 - Microsoft Server 2008/2012/2016
 - Microsoft Windows XP, 7, 8.1, 10
 - Linux Open Suse
 - Suse Linux Enterprise SLED, SLES
 - CentOS
 - Cameras from different manufacturers

No additional tools are required at runtime.

10. Edition of EuroPriSe Criteria used for the evaluation:

November 2011

11. Evaluation results:

With “vimacc” the manufacturer of the product offers a data protection friendly video management software. All data collected by video camera equipment is encrypted in the camera device. Transfer of video data is encrypted during transport. When storing data on the server the data is encrypted at rest. The data can only be decrypted by a user who has access to a hardware dongle that holds the private key for decrypting the data.

“vimacc” offers a comprehensive way of managing users and access rights for users.

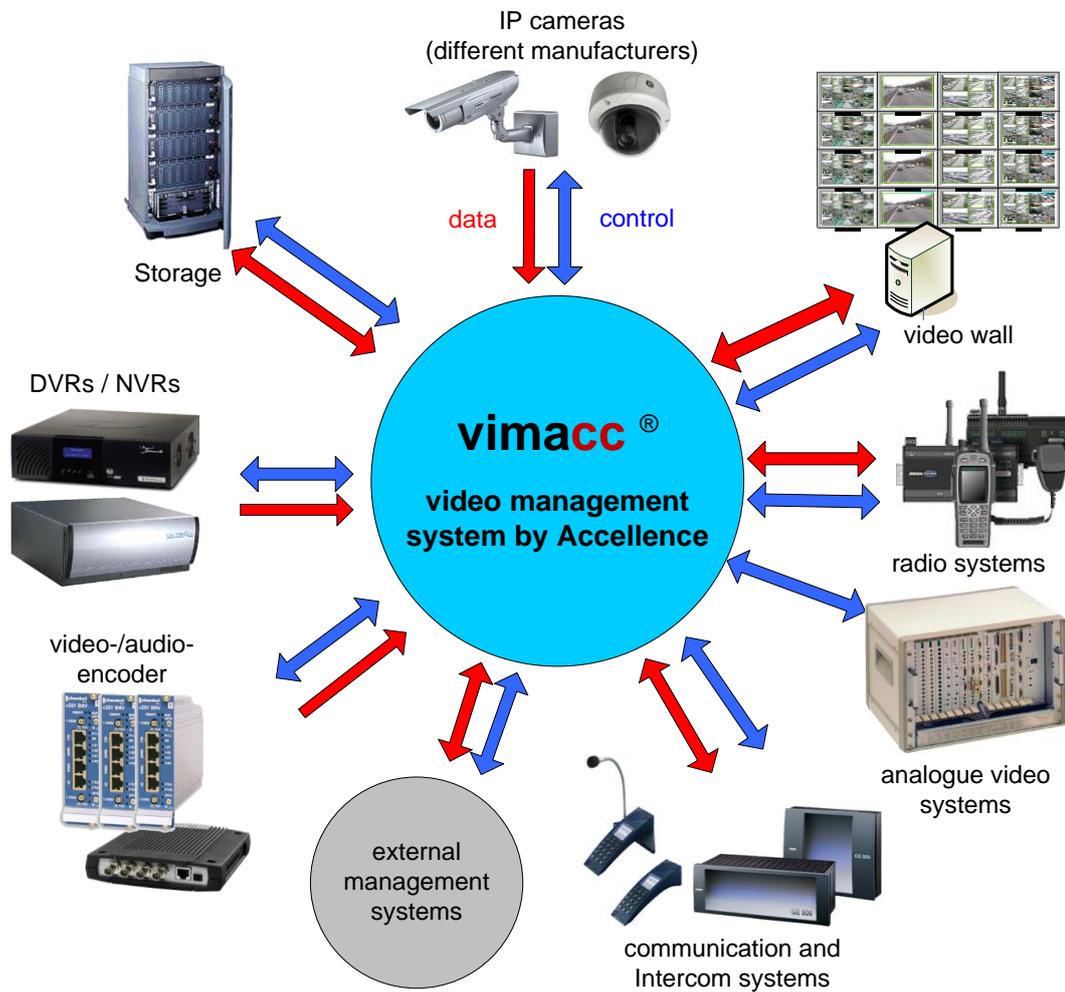
Another positive fact is, that the product offers data protection friendly options that allow for the pixelating of areas forming part of a video recording.

“vimacc” facilitates its privacy compliant use by its users who qualify as controllers regarding the video surveillance activities that are performed with the help of the ToE. However, the use of “vimacc” alone does not guarantee that a video surveillance activity complies with all relevant provisions of EU data protection law. Rather, the users of the service are required to assess the legitimacy of a video surveillance system prior to its deployment.

Accellence Technologies informs its customers on relevant privacy aspects in an exemplary manner by means of a data protection leaflet. This leaflet even provides the users of “vimacc” with a checklist that they can work through when planning the deployment of a video surveillance system.

Finally, it is to be highlighted that Accellence Technologies offers a specific licence model for “vimacc” that is tailored to the applicable EuroPriSe requirements and that ensures that the ToE is run under the restrictions that were already mentioned above at “6. Specification of Target of Evaluation (TOE)”. The users of “vimacc” are not capable of changing the implemented configuration.

12. Data flow:



13. Privacy-enhancing functionalities:

Encryption through the whole system, starting within the video-camera as an end-to-end encryption functionality.

14. Issues demanding special user attention:

None.

15. Compensation of weaknesses:

None.

16. Decision table on relevant requirements:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	<i>excellent</i>	The product makes extensive use of encryption technologies during transfer and storage of data. Furthermore, the product offers features that enhance privacy when using video surveillance technology. Areas of monitoring can be pixelated.
Transparency	<i>excellent</i>	The manufacturer does provide a comprehensive documentation of the product. Regarding data protection there is a specific manual that gives instructions for a data protection friendly use of the product.
Technical-Organisational Measures	<i>adequate</i>	The technical and organisational measures are excellent regarding some criteria (e.g., the role concept and multiple eyes principle). Some criteria had to be evaluated "adequate".
Data Subjects' Rights	<i>adequate</i>	A controller using the software can adhere to all provisions regarding data subject rights. The product does not support data subject rights in a specific way.

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Flensburg, 08.02.2017

Stephan Hansen-Oest



Place, Date

Name of Legal Expert

Signature of Legal Expert

Kellinghusen, 08.02.2017 Andreas Bethke



Place, Date

Name of Technical Expert

Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date

Name of Certification Authority

Signature