The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

# m.Doc GmbH
# Ursulaplatz 1
# 50668 Köln, Germany

to confirm that its technical procedures for video consultation

# Smart Health Video Service (Videosprechstunde)

fulfils all requirements of criteria

# Trusted Site Video Consultation, version 2.1

of TÜV Informationstechnik GmbH. The requirements are
summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation
report.

**Invalid from 2024-05-01**

Video Con-
sultation

**TÜViT** ®

2022 **Trusted Site**

Certificate ID: 5706.22

© TÜViT – TÜV NORD GROUP – www.tuvit.de

Certificate validity:
2022-03-30 – 2025-03-30

Essen, 2022-09-28

Dr. Christoph Sutter
Head of Certification Body

**TÜV Informationstechnik GmbH**

TÜV NORD GROUP

Am TÜV 1

45307 Essen, Germany

www.tuvit.de

TO CERTIFICATE

## Certification scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: "Zertifizierungsprogramm Trusted Site Video Consultation der Zertifizierungsstelle der TÜV Informationstechnik GmbH", Version 1.0 vom 2021-04-20, TÜV Informationstechnik GmbH

## Transfer note

The present certificate was issued by the certification body of TÜV Informationstechnik GmbH, which is already accredited according to ISO/IEC 17065 and is still in the accreditation process (including evaluation of the certification scheme) for an evidence according to §6 paragraph 2 letter a) of the agreement "Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V" as of October 21, 2016 in the version of February 25, 2021.

According to Annex 31b to the Federal Medical Insurance Contract (BMV-Ä) "Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V vom 21. Oktober 2016 in der Fassung vom 25. Februar 2021", this certificate may be used for a transitional period up to June 30, 2022, subject to any changes and extensions of the transitional period of Annex 31b to the Federal Medical Insurance Agreement (BMV-Ä).

The application number at the DAkkS is: PP-12-022-02.

## Evaluation report

The evaluation result is set out in the following report:

- German document: "Prüfbericht Trusted Site Video Consultation, Smart Health Video Service (Videosprechstunde)", version 1.1 as of 2022-03-23 TÜV Informationstechnik GmbH

## Evaluation requirements

- "Criteria Catalog Trusted Site Video Consultation", version 2.1 as of 2021-12-15, TÜV Informationstechnik GmbH.

The Evaluation Requirements are summarized at the end.

## Target of evaluation

- The target of evaluation "Smart Health Video Service (Videosprechstunde)" consists of the following components:

  - Android app, version 6.0.3099,

  - iOS app, version 6.12.3025 and

  - Web application, version 6.11.

The target of evaluation is an online video consultation in real time as part of a synchronous communication (peer-to-peer) between a doctor / alternative practitioner and a patient known to him.

Interfaces from the service providers Vonage / Tokbox are used so that the target of evaluation can implement the video consultation hour functionality according to the definition of the KBV. The use of the Vonage / Tokbox interfaces were also checked. The Vonage / Tokbox interfaces are not the responsibility of the manufacturer. Furthermore, the following

components are required to operate the target of evaluation, but are not part of it:

- Vonage / TokBox infrastructure components,

- m.Doc infrastructure components (e.g. Telekom Cloud Systems):

    o Network Load Balancer,

    o Databases.

## Evaluation result

- The target of evaluation fulfills the applicable requirements from the evaluation criteria catalog Trusted Site Video Consultation.

The recommendations given in the evaluation report must be observed.

## Summary of the evaluation requirements

### Technical and organizational measures

- The video service provider has defined security-relevant technical and organizational requirements for the operating environment of the video service and makes these available to the contracted doctor.

- The documentation of the necessary technical and organizational measures is easy to understand, suitable and comprehensible.

- The documentation is known to the contract physicians and is accessible at all times.

## 2 Network architecture

- The video service provider has documented the individual components of the video consultation and their security functions (architectural overview). The video consultation solution is structured in a meaningful and understandable way.

- The video service provider has provided information that identifies the security-relevant components and the interfaces of the product with their dependencies. Data flows (including the protocols used) are documented.

- The video service provider has documented appropriate hardening and protection measures.

- When deviating from a peer-to-peer procedure, suitable technical and organizational measures are defined to ensure an appropriate level of protection.

## 3 Encryption

All contents of the video consultation are encrypted according to the state of the art. The state of the art results in particular from the technical guideline 02102 of the Federal Office for Information Security in the currently valid version.

## 4 Storage of data

- The video service provider demonstrates and documents implemented measures for the storage or deletion of data. The video service provider does not view, save or pass on the content of the video consultation.

- The video service provider demonstrates through appropriate documentation and technical measures that

the metadata and technical connection data are deleted after three months at the latest and are only used for the processes necessary to process the video consultation.

## 5  Security risks

- The video service provider has provided evidence that penetration testing has been carried out (not older than 6 months) by an independent third party and which considered in particular the risks of the OWASP Top 10 catalog in the 2017 version.

- The report clearly shows the scope of the penetration testing and the components of the video consultation solution under consideration.

- It is clearly identifiable which test or attack procedures were used, so that it can be seen that the risks in the OWASP Top 10 catalog have been adequately examined.

- The video service do not have any exploitable serious vulnerabilities.