telemed.net Short Public Report

Application No. ULD080008p

1. Name and version of the IT product or IT-based service:

"telemed.net Version 2.11"

2. Manufacturer of the IT product / Provider of the IT-based service:

Company Name: telemed Online Service für Heilberufe GmbH

Address: Maria Trost 21, 56070 Koblenz, Germany

Contact Person: Oliver Harwart

3. Time frame of evaluation:

From March 2008 – November 2009

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

Legal Expert: Stephan Hansen-Oest

Address: Neustadt 56, 24939 Flensburg, Germany

Technical Expert: Andreas Bethke

Address: Papenbergallee 34, 25548 Kellinghusen, Germany

5. Certification Body:

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel
Germany
Tel +49-431-988-1200, Fax -1223
http://www.datenschutzzentrum.de
www.european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

Target of Evaluation is the product “telemed.net Version 2.11”.

The product offers a chat-function enabling direct communication between medical professionals.

The ToE includes:

- the application
- the server-hosting
- the interface to third party products

It does not include:

- client hardware
- third party products
- any parts of the MDIS (Medical Doctor Information System)
- further plugins.

7. General description of the IT product or IT-based service:

telemed.net is a product that offers a secured chat-function between medical professionals of different fields. The common use case is a one-to-one chat communication. However, the product supports chat communications with more than one communication partner. In any case the communication is encrypted symmetrically with an individually created key using the AES-192 encryption standard.

Furthermore the product provides a secured data file transmission between two medical professionals, who are only known by their patient but without a need to know each other.

8. Transnational issues:

All data processing occurs in a German data center. As telemed.net focuses on clients in the European Union the service is not geographically limited.

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

Java SE Development Kit 6
Eclipse 3.5 IDE
MS Visual C++
gnu C++
Apache Ant

10. Version of EuroPriSe Criteria for Experts used for the evaluation:

EuroPriSe Criteria Catalogue for Experts - Version 0.3

11. Evaluation results:

1. Secure Message-Handling

The product offers a chat-function, which gives the user (medical doctors) the possibility to directly communicate with other medical professionals of different fields by a so-called transport-encryption. The product is only offered to medical doctors and hospitals.

Telemed.net can be used alone, but it normally is used in connection with other software products (Medical Doctor Information Systems) via interface technologies. Main use case is the implementation of telemed.net into other Medical Doctor Information Systems (MDIS) as a white label solution. In practice MDIS has e.g. telemed.net technology implemented. All MDIS products that have implemented telemed.net ensure that only registered health professionals can use the product.

All messages are automatically encrypted before the message is submitted. Each message is encrypted with an individually generated key (AES 192) that transferred using a Diffie-Hellman key exchange and the public key (ECC 384) of the receiver. This encrypted key will be added to the encrypted message.
The public key is generated at the time of registration of a user and its public part is stored on a Server within the network. The private part of the key is stored on the system of the user.

Additionally the transport of the encrypted message is also encrypted via SSL. The transmission of the chat-data is carried out over the xmpp-ssl-Protocol. In case all chat-partners are online, messages are delivered immediately. If one partner is offline, messages are stored temporarily until the user is online again. In every case the messages are encrypted (ECC/AES) until decryption on the recipient's system. Messages are preserved until they are retrieved or until they are removed by deletion of the account.

The telemed.net user (medical doctor) may add other users to a “favourite-list”. Every product user is informed about the visibility of his or her data in advance. By using the general user list, one user may ask another user for consent to add him to his personal favourite-list. With the help of the list the user can administrate his or her communication-partners and gets information whether another user is on or offline. Except for the names, no further information of the participants is visible. Furthermore, users of telemed.net can enable an “online-history” of chat communication content. After enabling chat communication content will be stored and accessible for the user. Users can individually erase single or complete communication histories. The communication data is encrypted with individual public user keys (ECC-384/AES-192) to ensure that only the user can access this data unencrypted. By deleting an account all data (“online-history” included) will be removed - except for the user data (“Nutzungsdaten”). These user data (“Nutzungsdaten”) are needed for accounting and will be deleted after 6 months.

If a user is offline, messages are temporarily saved and will be delivered the next time the user is online.

2. Exchange of files

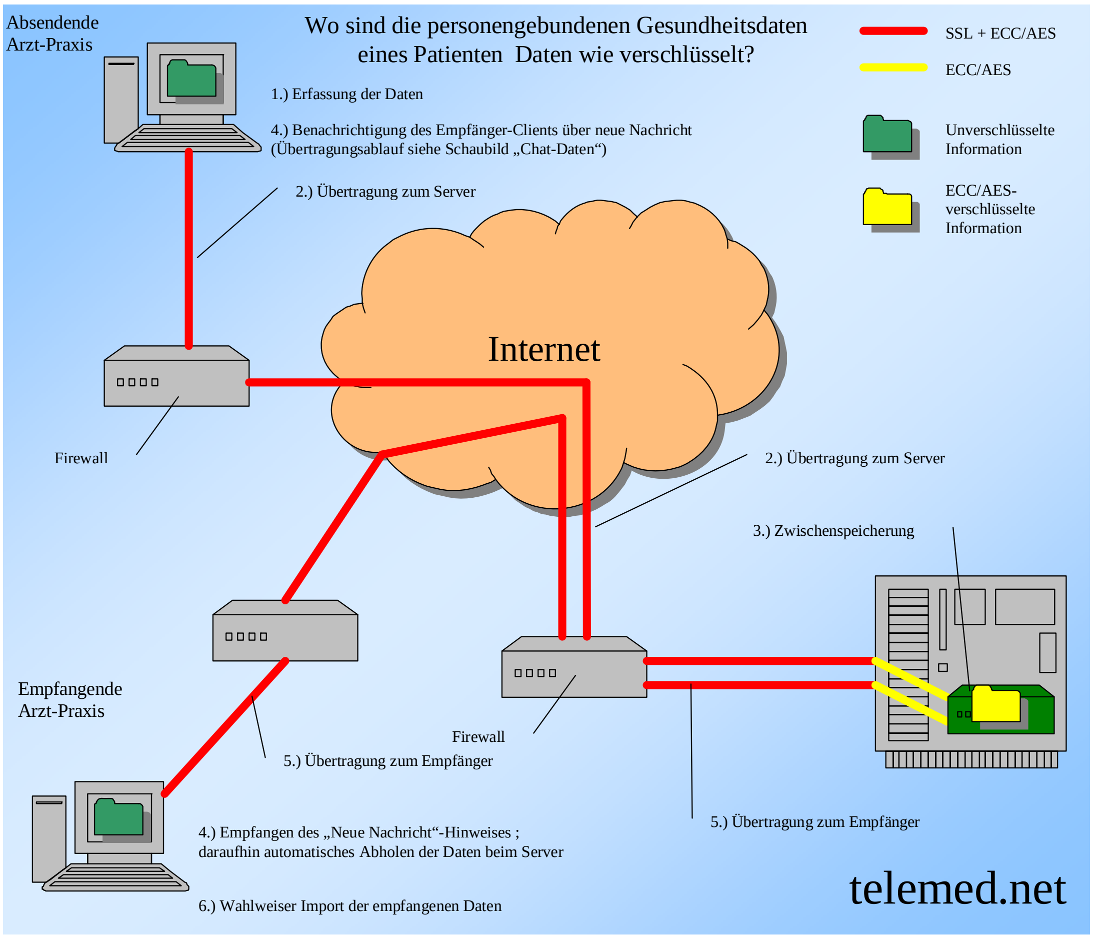
The second function of the product is the exchange of data in a file between users. The file-exchange modalities depend on the use of the MDIS which is not part of the target of evaluation. Instant Messages (IM) and documents are encrypted with the public key of the medical doctor receiving the file. The user controls any access and provides the access right to the receiver of the message or the document. In this case the second doctor is known by the first doctor.

Another possibility to exchange information is facilitated by the patient, as the receiving medical doctor might not be known at the time of sending the information. In this case, a medical doctor transfers selected medical information of a patient (from his MDIS) to another (unknown) doctor via telemed.net and paper documentation forwarded by the patient: As the “target-doctor” is not known by the first medical doctor, the patient receives a barcode (printed out on paper) and gives this to his chosen medical doctor, who can scan the barcode and decrypt the stored data with the help of this barcode and import the data into his MDIS.

For sending, the telemed.net-Client of the sender gets the information from the MDIS of the first medical doctor, encrypts it, build a barcode (which contains the key) and build a hash-value out of the barcode. This hash-value is the reference of the encrypted information to be stored on the telemed-server.

For retrieving and decoding the information, the receiving medical doctor scans the barcode he received from the patient. The telemed.net-Client takes this information, generates the hash-value, retrieves the encrypted information from the telemed.net-server, decrypts it (with the barcode) and passes the decrypted information to the MDIS. In this case the patient handles the access control.

12. Data flow:


Absendende
Arzt-Praxis
Wo sind die personengebundenen Gesundheitsdaten
eines Patienten Daten wie verschlüsselt?
SSL + ECC/AES
ECC/AES
Unverschlüsselte
Information
ECC/AES-
verschlüsselte
Information
1.) Erfassung der Daten
4.) Benachrichtigung des Empfänger-Clients über neue Nachricht
(Übertragungsablauf siehe Schaubild „Chat-Daten“)
2.) Übertragung zum Server
Internet
Firewall
2.) Übertragung zum Server
3.) Zwischenspeicherung
Empfangende
Arzt-Praxis
Firewall
5.) Übertragung zum Empfänger
4.) Empfangen des „Neue Nachricht“-Hinweises ;
daraufhin automatisches Abholen der Daten beim Server
5.) Übertragung zum Empfänger
6.) Wahlweiser Import der empfangenen Daten
telemed.net

13. Privacy-enhancing functionalities:

The product enhances privacy by the application of modern encryption technologies with the real time communication of data which are defeated by the medical oath of secrecy. It is in particular guaranteed that administrators of the communication server receive no knowledge from data which are defeated by the medical oath of secrecy. Furthermore, access control is in the hands of the patient.

14. Issues demanding special user attention:

The product generates a pair of private and public keys for the en- and decryption for each user. The public key is transferred to a communication server and the private key is transmitted to a medical information system. The product does not store the key pair, so the medical information system is responsible for the secured storage of the private key.

15. Compensation of weaknesses:

Does not apply

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	adequate	There is a minimisation of collecting primary data, which is strictly necessary for providing the service. For secondary data the convention of data avoidance and minimisation are fullfiled with the aid of the implemented “logrotation”-technique.
Transparency	adequate	All encryption-methods are described by telemed.net. The same applies to all technologies used or involved with the product. Telemed.net offers a user manual that gives a good overview on how the product can be used.
Technical-Organisational Measures	adequate	The technical-organisational measures taken by telemed,net to ensure the protection of data are adequate, though newest encryption methods are used which was evaluated excellent.
Data Subjects’ Rights	adequate	Regarding primary data of users of the TOE (doctors) there is sufficient information provided to the data subjects about the processing of their personal data. The product documentation and the product interface itself are transparent with regard of the data processing carried out with the product and service.

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.

Place, date Name of Legal Expert Signature of Legal Expert

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 security.

Place, date Name of Certification Body Signature