Quality of Life through Quality of Information
J. Mantas et al. (Eds.)
IOS Press, 2012

doi:10.3233/978-1-61499-101-4-512

Establishing End-to-End Security in a Nationwide Network for Telecooperation

Martin STAEMMLER[a,1], Michael WALZ[b], Gerald WEISSER[c], Uwe ENGELMANN[d], Robert WEININGER[e], Antonio ERNSTBERGER[f], Johannes STURM[g]
[a] *University of Applied Sciences, Stralsund, Germany*
[b] *Ärztliche Stelle für Qualitätssicherung in der Radiologie Hessen, TÜV SÜD Life Service GmbH, Frankfurt, Germany*
[c] *Radiologie und Geschäftsfeld Informationstechnologie und Qualitätssicherung, Universitätsmedizin Mannheim, Germany*
[d] *Chili GmbH, Dossenheim/Heidelberg, Germany*
[e] *pegasus gmbh, Regenstauf, Germany*
[f] *Abteilung für Unfallchirurgie, Universitätsklinikum Regensburg, Germany*
[g] *Akademie der Unfallchirurgie GmbH, München, Germany*

Abstract. Telecooperation is used to support care for trauma patients by facilitating a mutual exchange of treatment and image data in use-cases such as emergency consultation, second-opinion, transfer, rehabilitation and out-patient after-treatment. To comply with data protection legislation a two-factor authentication using ownership and knowledge has been implemented to assure personalized access rights. End-to-end security is achieved by symmetric encryption in combination with external trusted services which provide the symmetric key solely at runtime. Telecooperation partners may be chosen at departmental level but only individuals of that department, as a result of checking the organizational assignments maintained by LDAP services, are granted access. Data protection officers of a federal state have accepted the data protection means. The telecooperation platform is in routine operation and designed to serve for up to 800 trauma centers in Germany, organized in more than 50 trauma networks.

Keywords. Telecooperation, authentication, end-to-end security, trusted services, trauma

Introduction

High quality care of trauma patients requires cooperation from several involved centers, thereby extending over institutional boundaries. On the one hand use cases such as "second opinion", "clarification for transfer" or the "transfer" result from emergency situations. On the other hand subsequent treatment may lead to the following use cases: "rehabilitation", "physiotherapy" or "out-patient after-treatment".

Within the German Trauma Society (DGU) [1] more than 50 trauma-networks have been established representing 800 trauma centers. Trauma centers are entitled to apply for certification as local, regional and supra-regional trauma center according to

[1] Martin Staemmler, University of Applied Sciences, Stralsund, Medical Informatics, Zur Schwedenschanze 15, D-18435 Stralsund, Germany, martin.staemmler@fh-stralsund.de.

their compliance with structural and process quality criteria laid out by the whitepaper of the DGU [2] and monitored by means of a TraumaRegister® [3]. As such, the DGU has achieved a perfect organizational basis for telecooperation. However, when putting telecooperation into practice, each trauma network uses many different technological approaches for telecooperation, in particular to communicate treatment and image data. To avoid repetitive doubled effort the academy branch of the DGU (AUC) has setup a nationwide platform for telecooperation (TC).

The objective of this paper is to present the means taken for authentication, authorizations and end-to-end security compliant with data protection requirements legislation for guaranteeing privacy and at the same time supporting the functional requirements stated by the users.

1. Methods

Users' demands resulted in three levels of functionality (see Figure 1, left side) for the nationwide platform:

- TC-Basis provides a solely web-based access via a so-called web-viewer (available per download from the central infrastructure). Its functionality is limited to manual upload of treatment and image data dedicated for those entitled in the cooperating institution.
- TC-Router as a standalone application extends the above level by an automatic routing for DICOM objects after selection at a modality, a reporting station or a PACS.

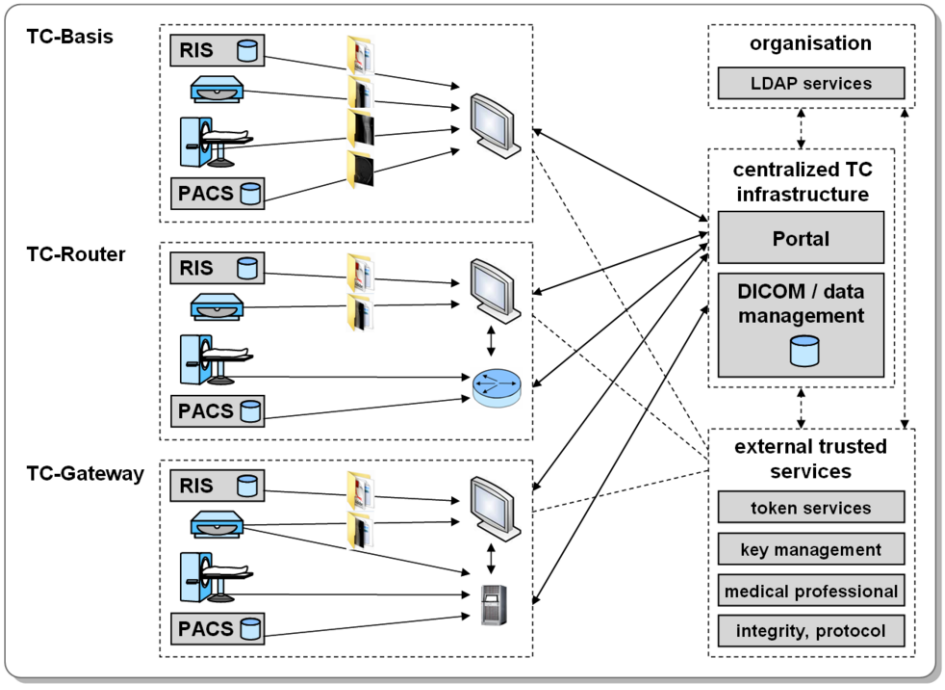

Figure 1. System architecture of the telecooperation platform.

- TC-Gateway allows for different approaches to reconciliation [4] by providing an intermediate PACS functionality for DICOM objects on top of the two previous levels. As such, it requires dedicated HW or a virtual machine environment for institutional implementation.

The implemented level at the receiving institution determines whether manual interaction (TC-Basis) provides image data or automation (TC-Router, TC-Gateway). Non DICOM data e.g. representing treatment information can be handled via the portal.

All software and hardware components used for the three levels are based on commercial products (CHILI GmbH, Germany) certified according to the Medical Device Directive (MDD) [5]. These have been integrated and extended to meet the project's requirements for messaging by means of the portal and transmission of non-DICOM data (such as requests, reports) assigned to DICOM objects. In addition, regulatory requirements have been addressed in a way to provide ease of use as well as to guarantee compliance.

1.1. Two-Factor Authentication

Besides the patient's consent, telecooperation requires identified individuals at the sending and receiving institutions. According to the German Federal Office for Information Security (BSI), individuals have to identify themselves using a two-factor authentication [6]. Since features such as fingerprint or iris scan are hardly usable in clinical practice, a combination of knowledge (login, password) and ownership (token for a one-time-password (OTP), mobileTAN) has been selected (Figure 2) and is mandatory to gain access from unsafe environments (e.g. at home, from mobile systems). However, within the safe environment of a medical institution, identified by its unique public IP address, access may be granted solely on the basis of login and password.

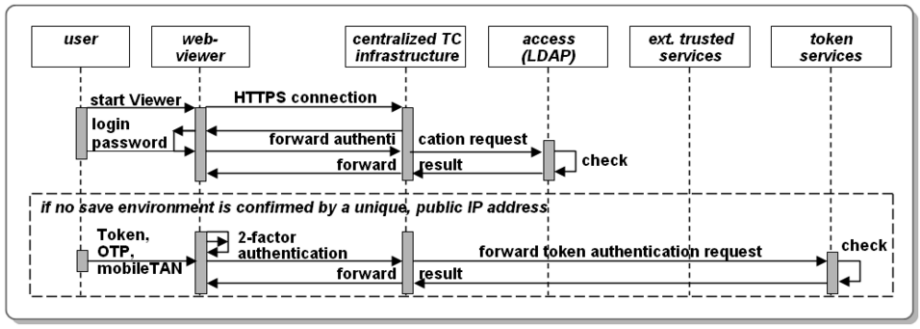

Figure 2. Two-factor authentication.

1.2. End-to-end security

Data privacy requires that only individuals involved in the treatment of the patient may gain access to patient data. However, for an emergency telecooperation request the medical doctor on duty might not be known. To remedy this situation the organizational hierarchy is provided by LDAP services and maintained by the trauma association and their authorized representatives. Based on this approach, data objects may be sent to a department but only an employee of that department is granted access.

Patient data is encrypted on application level using a symmetric key (AES 256) to support departmental addressing and to achieve end-to-end security. To protect the symmetric key from getting known by the infrastructure provider it is securely kept by independent external trusted services (Figure 1, right side). Life-cycle management of the key allows handling a potential corruption and involves resending previously transmitted data. The key is provided at runtime to the web-viewer (TC-Basis) or the applications (TC-Router, TC-Gateway) using a secured connection (SSL) together with a ticket to confirm successful authentication of a particular user and including a check for the user's role as a medical professional with the LDAP services.

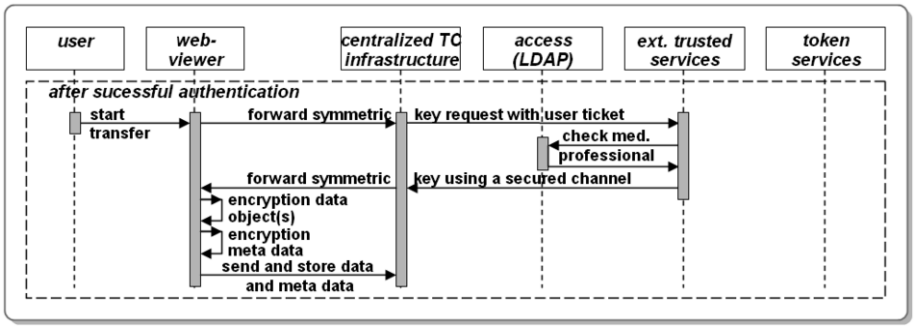

Figure 3. Encryption process using a symmetric key provided at runtime.

Since all data objects are kept encrypted associated meta data has be encrypted as well and stored additionally in order to avoid excessive download times for example for selecting data objects in the web-viewer.

1.3. Routine operation

A centralized topology is used to manage up to 800 institutions and to facilitate the web-based approach of TC-Basis. Its drawback as a single-point-of-failure is compensated by redundant systems and virtualization [7] for the centralized TC infrastructure, the LDAP services and the external trusted services. In addition, the external trusted services are responsible for audit compliant logging and application integrity checking.

All network communication is encapsulated within HTTP, HTTPS or email to avoid the need to open incoming ports on firewalls (e.g. for DICOM services).

2. Results

The portal implements the web-based services for all three functionality levels in combination with treatment and image data handling. Typical telecooperation use cases data reside only temporarily in the centralized infrastructure.

The platform is operational since autumn 2011 and is currently used in pilot trauma networks with ca. 100 trauma centers. Data protection officers of a federal state have accepted the data protection means. Besides some seed money from the AUC the trauma centers have contractually agreed to cover the costs for operating the platform and providing services such as help desk, monitoring and updates. Impact evaluation for trauma treatment will be achieved based on the existing TraumaRegister®. The

platform itself is prepared for further applications from other domains e.g. radiology, neurosurgery.

3. Discussion

In contrast to many established teleradiology networks this approach features three levels of functionality from a web-viewer up to a fully featured intermediate PACS for reconciliation.

End-to-end security for telemedicine has been presented on network level [8], with smart cards for individuals [9] or using a public-private-key infrastructure (PKI) [10]. A PKI incurs high maintenance cost. On the contrary, this approach is based on a symmetric key including a life-cycle management in case of corruption and a split responsibility between the system operator and contracted external trusted services together with the use of existing organizational structures.

Two-factor authentication has been a key demand requested by directives and guidelines [11] but nevertheless lacks implementation. The conditional approach taken in this nationwide network adapts to clinical and non-clinical settings while protecting patient data.

By including treatment data this approach is comparable to electronic case records [12], infrastructural services such as the IHE Cross Enterprise Document Sharing (XDS) [13] or future services of the national German eHealth infrastructure. However, these approaches typically require extensive effort to manage patient identity e.g. by means of a master patient index. Furthermore, specific application gateways or so-called connectors are needed for each institution and as such do not support a low-level web-based approach according to TC-Basis.

References

[1] www.dgu-online.de (last accessed 17.4.2012)
[2] Whitepaper Trauma Treatment, Deutsche Gesellschaft für Unfallchirurgie e.V., Berlin, http://www.dgu-online.de/pdf/unfallchirurgie/weissbuch/weissbuch.pdf (last accessed 17.4.2012)
[3] Probst C, Paffrath T, Krettek C, Pape HC and German Trauma Registry. Comparative update on documentation of trauma in seven national registries. Europ. J. Trauma 2006; 32: 357-364
[4] IHE Radiology Technical Framework, Volumes 1-3, Transactions, www.ihe.net, 2011
[5] European Parliament, Amendment to the Medical Device Directive, OJEC 2007; L247:21-55
[6] German Federal Office for Information Security (BSI), Measure M4.133, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m04/m04133.html, (last accessed 17.4.2012)
[7] Staemmler M, Service Delivery for e-Health Applications, User Centered Network Health Care, Studies in Health Technology and Informatics, IOS Press, Amsterdam, pp.533-541, 2011
[8] Wozak F, Schabetsberger T, Ammmenwerth E. End-to-end Security in Telemedical Networks – A Practical Guideline, Int. J. Med. Inform. 2007; 76: 484-490
[9] Alkhateeeb A, Singer H, Yakami M, Takahashi T. An End-to-End Secure Patient Information Access Card System, Method Inform Med. 2000; 39: 70-72
[10] Kurmann T, Slamanig D, Stingl C, Roessl K. Teleimage: An Integrated Approach for Secure and Web-based Exchange of Medical Images and Reports, IFMBE Proceedings 22, Springer, pp. 970-973, 2008
[11] Burr, WE, Dodson DF, Newton EM, Perlner RA, Polk WT, Gupta S, Nabbus EA. Electronic Authentication Guideline, National Institute of Standards and Technology, Publication 800-63-1. 2011
[12] Boehm O. eCR Application Architecture v1.2, www.fallakte.de/images/stories/pdf/spezifikationen/eFA1. 2-Anwendungsarchitektur-Normativ_v1.2.0.01.zip , (last accessed 17.4.2012)
[13] IHE Cross Enterprise Document Sharing (XDS), www.ihe.net, last accessed 17.4.2012)