Medical Informatics in a United and Healthy Europe
K.-P. Adlassnig et al. (Eds.)
IOS Press, 2009

doi:10.3233/978-1-60750-044-5-730

Securing a Web-Based Teleradiology Platform According to German Law and "Best Practices"

Michael SPITZER [1], Tobias ULLRICH, Frank UECKERT
Department of Medical Informatics and Biomathematics, University Hospital Muenster, Germany

Abstract. The Medical Data and Picture Exchange platform (MDPE), as a teleradiology system, facilitates the exchange of digital medical imaging data among authorized users. It features extensive support of the DICOM standard including networking functions. Since MDPE is designed as a web service, security and confidentiality of data and communication pose an outstanding challenge. To comply with demands of German laws and authorities, a generic data security concept considered as "best practice" in German health telematics was adapted to the specific demands of MDPE. The concept features strict logical and physical separation of diagnostic and identity data and thus an all-encompassing pseudonymization throughout the system. Hence, data may only be merged at authorized clients. MDPE's solution of merging data from separate sources within a web browser avoids technically questionable techniques such as deliberate cross-site scripting. Instead, data is merged dynamically by JavaScriptlets running in the user's browser. These scriptlets are provided by one server, while content and method calls are generated by another server. Additionally, MDPE uses encrypted temporary IDs for communication and merging of data.

Keywords. teleradiology, PACS, computer security, information storage and retrieval, confidentiality, internet

1. Introduction

Telemedicinal applications have become a matter of daily routine within the last years [1], resulting in increasing amounts of (probably highly) confidential data made available to physicians via network infrastructures. Since, as the transport layer, the Internet is utilized more frequently [2], operators of such health telematics platforms have to take special care to ensure confidentiality of data and privacy of patients [3].

As a teleradiology platform, the Medical Data and Picture Exchange platform (MDPE) handles both identity and diagnostic data. In Germany, data security and confidentiality, especially in the context of health telematics, are very prominent and obligatory topics. It has thus become standard practice to develop specific data security concepts for telemedicine applications, describing utilized software components as well

[1] Corresponding Author: Michael Spitzer, Department of Medical Informatics and Biomathematics, University Hospital Muenster, Domagkstrasse 11, 48149 Muenster, Germany; E-mail: spitzer@imfl.de.

as data collection, storage and distribution. Concepts are critically discussed, evaluated and certified by German data security authorities and recommended for deployment.

MDPE offers a teleradiology service as a web-based platform. To allow users to efficiently exchange medical data via the Internet, the underlying complex data security concept shall not inflict restrictions or aggravations onto the user. Otherwise, the platform's acceptance by physicians would be poor and possible benefits of incorporating an online telemedicine platform into daily routine would be undone by secure, yet complex workflows. The following sections describe MDPE's features and security measures, among which is a sophisticated JavaScript-based framework (cf., section 4) for merging data from different sources within the web browser.

2. MDPE Feature Overview

MDPE supports the secure exchange of primarily medical imaging data in the DICOM format [4, 5] via the Internet by integration of Open-Source software and libraries (Offis DICOM toolkit [6], MedCon [7], PixelMed toolkit [8]). Using custom Java applets running within a user's web browser, MDPE allows the upload of whole DICOM CDs, as well as sending and receiving DICOM objects via the DICOM-STORESCP protocol.

Access to patient data and corresponding documents is regulated via an extensive role model, allowing for fine-grained configuration of roles on the basis of privileges linked to functional modules. Each privilege can be enabled or disabled for a specific role. Access to patients can be propagated by one user to other users by an integrated booking system, mimicking the workflow of traditional referrals.

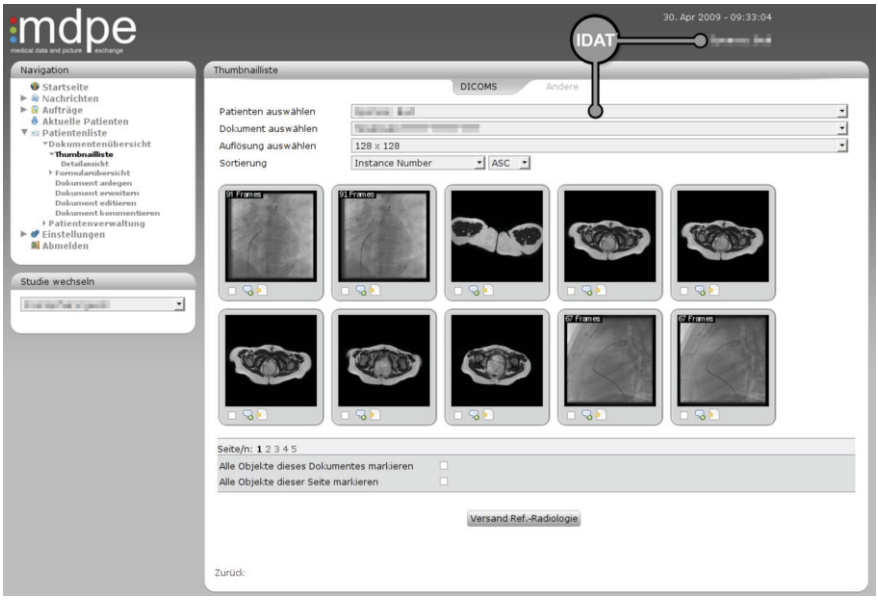

Figure 1. In this thumbnail view the patient's name, as displayed by a SELECT box and a DIV area (both marked by "IDAT"), is provided by a logically and physically separate web server and dynamically merged into the HTML document by the user's web browser using short JavaScript method calls.

3. Data Security Concept

Besides using encryption for storage and communication, the risk of eavesdropping and abuse of patient data is minimized by the implementation of a generic data security concept developed and provided freely by the German Telematics Platform for Medical Research Networks (TMF e.V., [9]). This concept, although not codified in binding national or European law (e.g., directive 2002/58/EC), is already generally accepted as "Best Practice in Data Security" among German authorities and features a strict logical and physical separation of identity (IDAT) and diagnostic (MDAT) data (cf., Figure 2). This separation scheme is established in Germany by now insofar as data security concepts of medical research networks not implementing this particular separation of data classes often find themselves required justifying their own deviation in detail.

The combination of both data classes (IDAT and MDAT) in a single location other than the authorized physician is considered a serious threat for a patient's privacy. In case of theft (or eavesdropping) the invading party would gain straightforward access to whole patient files including name, address as well as diagnostic records, making abuse easy.

The generic TMF concept was adapted to the specific conditions of web-based platforms, retaining the consistent data separation scheme. This specific concept was positively accredited by both the TMF and data security authorities. As a consequence, IDAT and MDAT may exclusively be merged at authorized clients. Deliberate or accidental merging of both data classes by central MDPE components is considered an inacceptable deviation from the data security concept and thus a serious security breach.

Data is stored pseudonymously in all cases [10], implying that IDAT and MDAT reside on logically and physically separate servers, located in different data centers and maintained by different administrators. Upon upload, all identifying information is removed from data objects and stored in relation to a random code (i.e., the pseudonym). This procedure primarily affects DICOM objects, as all header fields containing identity information are discarded (a patient's identity data is already stored in the IDAT database). Statistically important data (e.g., weight, age) are preserved.

The IDAT and MDAT classes each contain mutually exclusive data only, except for a single item: the PID (an internal patient ID). Its sole use is to associate corresponding IDAT and MDAT records. As misuse would be straightforward if the PID was publicly known (by simply linking an MDAT record to a patient's identity) it is vital to confine it to the system. Thus, to communicate with the "outside" world, random temporary IDs (TempID) are used. When a user requests data, a TempID is stored in relation to that request and simultaneously announced to the client for further communication. After usage, or after a specific grace period as fallback, the TempID is automatically invalidated. In this way no permanent IDs are revealed and the risk of security breaches is minimized.

4. Results: Dynamic Merging of Data by Encrypted JavaScriptlets

MDPE implements a custom JavaScript framework for the dynamic generation and placement of content (cf., Figure 1 for an example view of the graphical user interface). When users request views which combine e.g., digital imaging data and, in some portion of the layout, patient identity information, the MDAT server embeds the JavaScript base library within the dynamically generated HTML code. This library

provides various sophisticated methods for automatically filling e.g., DIV blocks or various form elements (such as SELECT boxes, TEXT fields, etc.) with IDAT content *after* the MDAT content was already delivered to the user (cf., Figure 2).

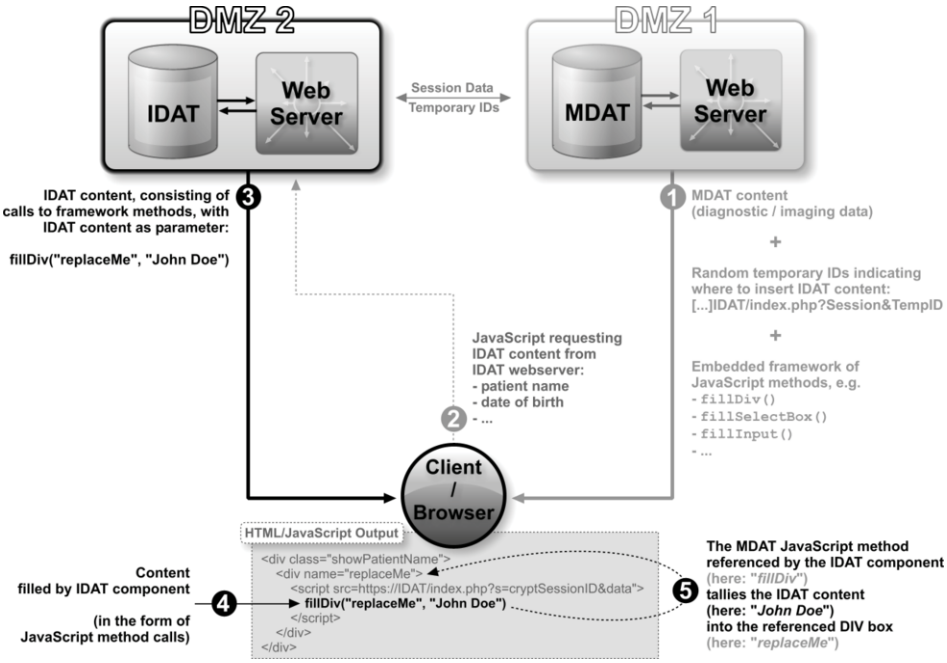

Figure 2. Depiction of the merging of IDAT content into an HTML page. The HTML code is prepared and delivered to the client by the MDAT component from within a separate DMZ (i.e., demilitarized zone). The individual steps, starting with the delivery of MDAT content including the JavaScript framework, are indicated by circled numbers with descriptive text attached. MDAT content and the client's requests to the IDAT server are colored in medium gray, whereas IDAT content is indicated in black.

Content which is to be replaced or supplemented is marked in the HTML delivered by the MDAT server by temporary random IDs. The MDAT server dynamically generates short JavaScriptlets, which are executed automatically on page load and call a PHP script on the IDAT server. As GET parameters this script is provided with the encrypted session ID as well as the temporary IDs generated above and a task description (e.g., "fill in patient name into DIVs").

Sessions reside in a database and are accessible by both the IDAT and MDAT servers in order to allow checking the authentication status of a user. Based on the (decrypted) session ID and the temporary IDs, the IDAT server is able to retrieve IDAT data for the requested patient from its database.

The IDAT server then returns dynamically generated JavaScript code, simply consisting of calls to the already existing JavaScript methods of the framework (which was loaded from the MDAT server) and providing the requested content as parameter to the method (e.g., patient name, date of birth). The code is executed in the user's browser and tallies the IDAT data into a document's DOM structure [11] by utilizing the JavaScript functions that have already been pre-defined by the MDAT component.

In the end, users are presented with a document view that appears to be forged by a single server, without requiring them to deal with complex topics of web-based

telemedicine such as pseudonyms by themselves. “Behind the scenes” the content was transparently merged from different sources, as demanded by “German Best Practices”. The performance hit caused by dynamically inserting content from different sources via JavaScript methods is marginal and normally not noticeable by the user. Moreover, the JavaScript framework is scalable, in order to enable merging of data not only from two but from multiple sites, if advised and required in specific scenarios.

5. Conclusion

The criticism, that increasing data security requirements and therefore increasingly complex applications hamper the user’s acceptance of health telematics applications, thus diminishing putative positive effects on efficiency of information exchange and a patient’s health care quality in the long run [12], has been averted by MDPE.

Since diagnostic data, in agreement with the generic TMF data security concept, is strictly separated from identification data, the Medical Data and Picture Exchange platform fully complies with state-of-the-art requirements and standards established by German authorities. These latest standards are not yet determined as federal or European law but expected by local data security authorities on the basis of data security concepts individually written and evaluated for specific use cases and thus individual national medical research networks.

By implementing a versatile JavaScript framework for the dynamic placement of patient identity information in HTML content, the MDPE platform represents a modern and interactive web-based telemedicine application. By utilizing up-to-date dynamic techniques of the so-called Web-2.0 era the user is provided with an easy-to-use and responsive graphical user interface to the underlying complex telematics infrastructure.

References

[1] Knaup, P., Bott, O., Kohl, C., Lovis, C., Garde, S. (2007) Electronic patient records: Moving from islands and bridges towards electronic health records for continuity of care. *IMIA Yearbook of Medical Informatics 2007*, 34–46.
[2] Münch, H., Engelmann, U., Schröter, A., Meinzer, H.P. (2004) The integration of medical images with the electronic patient record and their web-based distribution. *Academic Radiology* 11(6):661–668.
[3] Blobel, B., Pharow, P. (2007) Security and privacy issues of personal health. *Studies in Health Technology and Informatics* 127:288–297.
[4] Parisot, C. (1995) The DICOM standard. A breakthrough for digital information exchange in cardiology. *International Journal of Cardiac Imaging* 11(Suppl 3):171–177.
[5] Bidgood Jr., W.D., Horii, S.C. (1992) Introduction to the ACR-NEMA DICOM standard. *Radiographics* 112(2):345–355.
[6] http://dicom.offis.de/dcmtk.
[7] Nolf, E., Voet, T., Jacobs, F. et al. (2003) XMedCon – An open-source medical image conversion toolkit. *European Journal of Nuclear Medicine* 30(Suppl 2):S246.
[8] http://www.pixelmed.com/#PixelMedJavaDICOMToolkit.
[9] http://www.tmf-ev.de/.
[10] Pommerening, K., Miller, M., Schmidtmann, I., Michaelis, J. (1996) Pseudonyms for cancer registries. *Methods of Information in Medicine* 35(2):112–121.
[11] Brelstaff, G., Moehrs, S., Anedda, P., Tuveri, M., Zanetti, G. (2001) Internet patient records: New techniques. *Journal of Medical Internet Research* 3(1):E8.
[12] Hebert, M. (2001) Telehealth success: Evaluation framework development. *Studies in Health Technology and Informatics* 84:1145–1149.