Volume 50 · Supplementary vol 1 · Part 2 **2005**

Biomedizinische Technik

Organ of the German Society for Medical and Biological Engineering within VDE, Swiss and Austrian Societies for Biomedical Engineering

Publishing Company:

Fachverlag Schiele & Schön GmbH,
Markgrafenstraße 11, 10969 Berlin (Germany)
Telefon +49-30-253752-0, Fax +49-30-25172 48

Medical Physics

Proceedings of the jointly held Congresses

ICMP 2005

14th International Conference of Medical Physics of the International Organization for Medical Physics (IOMP), the European Federation of Organizations in Medical Physics (EFOMP) and the German Society of Medical Physics (DGMP)

BMT 2005

39th Annual Congress of the German Society for Biomedical Engineering (DGBMT) within VDE

14th - 17th September 2005
Nuremberg, Germany

Editorial:
W. Kalender
E. G. Hahn
A. M. Schulte

ISSN 0939-4990

Fachverlag Schiele & Schön GmbH
Markgrafenstr. 11, 10969 Berlin (Germany)
Telefon: +49-30-25 37 52-0
Telefax: +49-30-25 37 52-99

This supplement is not part of the journal „Biomedizinische Technik“ and is published beyond the editors and publishing company’s responsibility.

The responsible editors for this supplement:
W. Kalender
E. G. Hahn
A. M. Schulte

Printed in Germany

Track 9 Information Technology / Health System Economics.....1454

Analyzing foot pressure distribution in patients with total knee endoprosthesis (TEP) using pattern recognition techniques
C. Schuld, R. Rupp, G. Ochs, H.-G. Simank, H. J. Gerner, M. Schablowski-Trautmann, Heidelberg, Germany.....1454

Principal Component Analysis for Microcalcification Selective Enhancement in the Wavelet Domain
L. Costaridou, N. Arikidis, P. Sakellaropoulos, S. Skiadopoulos ,G. Panayiotakis, Patras, Greece 1456

Time independent simulation of blood flow by CFD after heart valve replacement
M. Bongert, M. Geller, Dortmund, Germany.....1458

An electronic tool for multi-center administration, assessment and analysis of clinical trials in spinal cord injury
R. Rupp, J. Schweidler, A. Curt, V. Dietz, H.-J. Gerner, Heidelberg, Germany 1460

The Public Key Infrastructure of the Radiological Society of Germany
B. Schütze, P. Mildenberger, G. Klos, M. Kämmerer, Mainz, Germany.....1462

Teleradiology according to the German “Röntgenverordnung” - exemplary application of the Open Source Software “SecTelMed”
B. Schütze, P. Mildenberger, G. Klos, M. Kämmerer, Mainz, Germany.....1464

Parsing XML documents with medical content on mobile phones
J. Orlowski, K. Biskup, B. Jettkant, B. Clasbrummel, Bochum, Germany.....1466

Context-aware personal health monitoring using body wearable sensors
C. Kunze, W. Stork, K. Müller-Glaser, Karlsruhe, Germany 1468

Web based quality assurance tools for special treatment techniques in radiotherapy: An intranet application for QA of total body irradiation under translation conditions
J. Licher, U. Ramm, J. Moog, F. Rudolf, H.-D. Böttcher, S. Mose, Frankfurt/Main, Germany 1470

e-Ophthalmology for clinical decision support
S. Kurapkiene, A. Paunksnis, V. Barzdziukas, Kaunas, Lithuania 1472

A Smartphone based application for HRV analysis
L. Moraru, R. Strungaru, Bucharest, Romania.....1474

Development of a Bipolar Forceps Prototype for Electrosurgical Ablation Procedures in the Cardiac Atrium for the Intra-Operative Treatment of Atrial Fibrillation 1476

The Public Key Infrastructure of the Radiological Society of Germany

B. Schütze[1)], M. Kämmerer[1)], G. Klos[1)], P. Mildenberger[1)]

1) Johannes Gutenberg-University of Mainz - Department of Radiology, Mainz, Germany

Abstract

PGP (Pretty Good Privacy) encoding is based on the Public Key Procedure and permits the safe transmission of medical data. Furthermore it allows the use of an electronic signature provided that used keys belong to the key owner and that the key owner's identity is guaranteed by a trusted third party. Under the auspices of the Radiological Society of Germany (Deutsche Röntgengesellschaft, DRG) its IT-Working Group (Arbeitsgemeinschaft für Informationstechnik, @GIT) build up an appropriate Certification Authority including the required Public-Key-Infrastructure. These @GIT certified PGP keys allow the legal use of telemedicine in Germany. Digital signatures based to those certified keys correspond to the advanced signature according to the German signature law.

1 Purpose

In Germany patients' data must be encoded before transferring [1]. A Public-Key-Infrastructure (PKI) is an essential condition for a safe and legally incontestable usage of the available cryptographical solutions. As a side effect that one leads the use electronic signature, presupposed integration into the radiological Workflow, for a faster availability of the diagnostic reports for the referring physicians [2].

Up to now any system providing physicians with a qualified signature is not existing in Germany. Projects to establish a 'patient's card' and a 'health professional card' are still under planning. According to existing time schedules it will be introduced not before 2006. Several IT-experts had already expressed their doubts about keeping that schedule, though. However, establishing a 'health card' without qualified signature is conceivable yet, as long as this item will be provided later on. Since there is actual need for a basic infrastructure as prerequisite for telematic applications, a PGP-based PKI initiative under the auspices of the DRG had been founded at the "85th German Radiography Convention".

2 Materials and Methods

The PGP encoding is based on the Public-Key-Method. Any user has got at least two keys, one public key and one secret key. The public key is available for potential communication partners, the secret key must be protected against the access of third parties.

The data will get encoded with the public key of the communication partner and can only be decrypted by using the secret key of the addressee.

The sender uses his private key to create the digital signature as follows:

1. A Hash-function creates a 'fingerprint' of the electronic document.
2. This 'fingerprint' is encoded with the private key of the signer, using an asymmetrical proceeding (best known is RSA).

The encoded fingerprint is the digital signature. Verifying the signature requires the signature itself, the original data and the public key. At first the signing procedure is reverted and the signature decoded with the public key, thus getting the Hash-value which is included in the key. Since Hash-functions are one-way-functions it is not possible to get the original data that way, but out of the attached original data the Hash-value is generated. This newly won Hash-value is compared with the transmitted Hash-value. If both values match, the digital signature is authentic.

To ensure the authenticity of keys and confirm the identity of the attached person, the public keys can be signed by third persons/institutions. A key which had been signed by a trustworthy person or institution (and which had not been voided, meanwhile) is trustworthy, and the attachment of the person/institution named in the key to that key is granted. This mechanism of mutual signing and confiding forms the so-called "web of trust".

However, in Germany data (e.g. clinical findings) which are solely transferred via the "web of trust" are not considered legally equal to those conventionally signed by hand. According to the German Signature Law, achieving such legal equality requires the application of a so-called "Qualified Signature". This signature may be issued and administered only by qualified institutions ("Trust Centers"). Only individual-related signatures are accepted, though. Furthermore their validity is temporarily limited to 5 years and they have to be stored for at least 30 years. All this results in relatively high costs.

Alternatively an own public-key infrastructure (PKI) can be set up. According to state-of-the-art technology, PKI is a method which grants authentication, identification, confidentiality and unambiguity of electronic data – in this way creating an infrastructure to issue and administer cryptographical keys [3]. Thus the attachment of key to a certain person is granted [4].

3 Results

Since there is actual need for a safe telecommunication, the German Association of Radiology (DRG) determined to act as certificate authority (CA) and to guarantee the positive attachment of key to key owner. For this the DRG signs (and even offers the possibility to create, if demanded) private PGP-keys at public events (e.g. the German Radiology Convention and the DICOM-meeting). The CA of the DRG is operated by its IT-Working Group (Arbeitsgemeinschaft für Informationstechnik, @GIT).

Thus DRG, respectively @GIT, created a Public-Key-infrastructure (PKI). According to state-of-the-art technology, PKI is a method which grants authentication, identification, confidentiality and unambiguity of electronic data, in this way creating an infrastructure to issue and administer cryptographical keys [3]. The Public-Key-Infrastructure forms a technical basis of telemedicine [5]. Without it a confidential, protected and legally obligatory communication between hospitals, medical practices, patients et al is not possible.

To make the required public keys available to communication partners, the DRG set up a "PGP key server" on the Internet (http://www.radiologie-informatik.de/keyserver/). The key-server is an Open-Source-product (PKS, http://pks.sourceforge.net/) which is used by the "Computer Emergency and Rescue Team" of the German Research Network (Computer-Notfall-Team für das Deutsche Forschungsnetz, DFN-CERT), too.

The keys signed by the DRG or @GIT fulfil the demands of advanced signature according to § 2, 1 (2) of the German Signature Law:

1. The signature is exclusively attached to the key owner.
2. The keys had been produced by procedures which are exclusively under the key owner's control.
3. The identification of the signature-key-owner is granted.
4. The data, to which the keys are referring, are combined in a way that "subsequent modifications are detectable."

These demands are fulfilled:

1. Personal data and PGP-Public-Key-data are noted down on the certification application form and signed after the presentation of an official identification paper.
2. The keys created by @GIT were produced with a special PC without possibility to store or manipulate data.
3. The signing of the keys with the @GIT-key only was done after the presentation of identification card or passport, hence the DRG guarantees the key owner's identity.
4. Because of the @GIT-key-signature subsequent alterations of the key become obvious at any time.

PKI-created advanced signatures are legally equivalent to the handshake of daily life.

4 Discussion

Even though only the qualified signature, respectively the qualified signature with supplier accreditation, is absolutely equivalent to the signing by hand, according to various lawyers the advanced signature fulfils more than 90% of the requirements.

With its activities the initiative of the DRG has taken an important step to the utilization of telematic applications in health care. Based on its results other projects (e.g. the Teleradiology-Initiative of @GIT) can be carried out and find their way into the medical workflow.

It is desirable that further professional associations or Medical Boards join the initiative of the DRG or at least set up their own corresponding compatible structures. Thus, without much effort, the legally incontestable foundations for the usage of telematic applications could be laid. Probably these infrastructures will have raison d'être even after the establishment of HPC, since HPC does not allow encoded transmission of patients data abroad, due to the lack of corresponding infrastructures on the opposite side.

5 References

[1] Mand E. Datenschutz in Medizinnetzen. MedR 2003; 7: 393-400.

[2] Lepanto L. Impact of Electronic Signature on Radiology Report Turnaround Time. Journal of Digital Imaging, 2003; 16 (3): 306 – 309

[3] He Q, Sycara K, Su Z A Solution to Open Standard of PKI. LNCS 1998; 1438: 99–110.

[4] Müller S, Müller WB. The Security of Public Key Cryptosystems Based on Integer Factorization. LNCS 1998; 1438: 9-23

[5] Brandner et al.. Electronic Signature for Medical Documents – Integration and Evaluation of a Public Key Infrastructure in Hospitals. Methods Inf Med 2002; 41: 321-330

Corresponding author: Dr. Bernd Schütze
E-Mail address: schuetze@medizin-informatik.org