Erik-Oliver Blaß

Analyse, Verifikation und Realisierung kryptographischer Protokolle fuer flexible Zugriffe auf medizinische Datenbanken

Diplomarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 2001 GRIN Verlag
ISBN: 9783638130981

Erik-Oliver Blaß

Analyse, Verifikation und Realisierung kryptographischer Protokolle fuer flexible Zugriffe auf medizinische Datenbanken

GRIN Verlag

Diplomarbeit

Analyse, Verifikation und Realisierung kryptographischer Protokolle für flexible Zugriffe auf medizinische Datenbanken

Universität Karlsruhe
Fakultät für Informatik
Institut für Algorithmen
und Kognitive Systeme

Erik-Oliver Blaß

Betreuer: Prof. Dr. Thomas Beth
Betreuender Mitarbeiter: Dipl. Inform. Jörg Moldenhauer

8. Oktober 2001

Erklärung

Ich versichere, diese Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben.

Karlsruhe, den 8. Oktober 2001

(Erik-Oliver Blaß)

Kurzfassung

Der Umgang mit sensiblen Patientendaten stellt hohe Anforderungen an deren Vertraulichkeit und Integrität. Für einen entfernten, elektronischen Zugriff auf solche Daten und deren elektronische Verarbeitung sind besondere Sicherheitsvorkehrungen nötig, um Geheimhaltung und Schutz vor Mißbrauch zu gewährleisten. Ein Problem dabei sind insbesondere die zeitlich veränderlichen Zuständigkeiten und Verantwortlichkeiten für Patientendaten im klinischen Alltag.

In dieser Arbeit werden auf bestehenden kryptographischen Komponenten basierende Protokolle zum Zugriff auf medizinische Daten entwickelt, die diese Anforderungen gezielt umsetzen. Dazu gehören die gesicherte Speicherung der medizinischen Daten in speziell hierfür entwickelten Datenbanken sowie eine funktionsspezifische Rechtverwaltung und Zugangskontrolle mittels sogenannter Rollen.

Die erarbeiteten Protokolle und das Umfeld ihres Einsatzes werden auf verschiedenen Ebenen analysiert und ihre Sicherheit formal bewiesen. Mit einer Implementierung in Java wird die Einsatzfähigkeit der Protokolle gezeigt. Die Verwendung von CORBA-Kommunikationsmechanismen erlaubt die Einbindung in ein verteiltes medizinisches Informationssystem, das vom IAKS im Rahmen des Teilprojekts Q6 des SFB 414 „Informationstechnik in der Medizin“ als Prototopy entwickelt wird.

Inhaltsverzeichnis