Grundsätzliches

Die Arbeitsgruppe „Institut für Telematik“ ist ein Forschungs- und Entwicklungszentrum, die ehemals von der Fraunhofer-Gesellschaft betreut wurde. Es wurde am 1. Januar 1998 gegründet und entwickelte sich zum Kompetenzzentrum für anwenderfreundliche und praxistaugliche Hightech-Lösungen auf dem Gebiet, wo Telekommunikation und Informatik miteinander verschmelzen. Es beschäftigt ca. 30 Wissenschaftler verschiedener Disziplinen und Nationalitäten.

Das Tätigkeitsspektrum reicht von der anwendungsorientierten Forschung in den Bereichen Telekommunikation und Informatik bis zur Entwicklung maßgeschneiderter Hightech-Lösungen und Pilotsysteme für Wirtschaft, Medizin und Verwaltung. Darüber hinaus ist es auch in der Aus- und Weiterbildung tätig: Sowohl Kooperationspartner als auch interessierte Mitarbeiter von Unternehmen werden mit den sogenannten neuen Medien vertraut gemacht.

Projektpartner

Projektpartner des Instituts sind neben High-Tech-Unternehmen und Großbetrieben vor allem auch klein- und mittelständische Firmen, in denen die wissenschaftlichen Ergebnisse in die betriebliche Praxis umgesetzt werden. Die Tätigkeitsschwerpunkte liegen insbesondere in der Entwicklung und Nutzung neuer Informations- und Kommunikationsmedien in Wirtschaft, Technik, Medizin und Gesellschaft.

Kompetenzbereiche

Die derzeitigen Forschungs- und Entwicklungsprojekte sind darauf gerichtet, die neuesten wissenschaftlichen Entwicklungen in den Bereichen Internet/Intranet, sichere Datenübertragung, Telemedizin und elektronisches Publizieren praktisch nutzbar zu machen. Das Institut ist dabei insbesondere auf folgenden Feldern tätig:

- Redaktionssysteme: webbasiertes Informations- und Knowledge-Management
- Navigationssysteme: Aufbereitung von Informationen, Datenbank-Schnittstellen, EAI, Data Warehouse
- Datenbankmanagement: Innovative Middleware auf der Basis offener Standards, z.B. Smart Data Server (SDS)
- Sicherheit in offenen Netzen: Architekturen, Policies
- Sicherheit von Netzwerken: Firewalls, Lock-Keeper, Tiger Teams, CERT
- Sicherheit von Inhalten: Public-Key-Infrastrukturen, Digitale Signaturen
- Mobile Technologien und Anwendungen: Ubiquitous Computing, Mobile Security, ad hoc-Netze, Smart Cards
- Telemedizin: Patienten-CD, DICOM-Bildmanagement und -komprimierung,
- Consulting: Studien, Gutachten, Audits

Patentschutz erhielt das Institut bereits für zwei Lösungen: den „Lock-Keeper“, eine Sicherheits-„Schleuse“ zwischen Internet und Intranet, die sicherer als Firewalls gegen Online-Attacken schützt und das Bildkomprimierungs-Verfahren „Dicomzip“, das die Übertragungszeit medizinischer Bilder von mehreren Stunden auf wenige Sekunden senkt.

Universität-Trier

Institut für Telematik

Hightech-Forschung rund ums Internet

elektronisches Studienbuch

Sicherheitsaspekte einer virtuellen Universität

Bahnhofstr. 30-32
54292 Trier, Germany
Telephone: +49 (0) 651 - 97551 - 0
Telefax: +49 (0) 651 - 97551 - 12
E-Mail: info@telematik-institut.de
Internet: http://www.telematik-institut.de

Leitung:
Univ.-Prof. Dr. sc. nat. Christoph Meinel

Elektronisches Studienbuch - Sicherheitsaspekte einer virtuellen Universität

Seit einigen Jahren werden Ideen und Konzepte rund um virtuelle Hochschulen verstärkt entwickelt. Der Hintergrund liegt hierfür in der zunehmenden Verfügbarkeit von Computern mit multimedialen Fähigkeiten für breite Bevölkerungsschichten. Der Zugang zum World Wide Web ist für viele zur Selbstverständlichkeit geworden. Um eine virtuelle Universität jedoch zu verwirklichen, bedarf es nicht nur des Verständnisses über die Lerninhalte und das Zusammenwirken der verschiedenen Komponenten, die das Lernen über Entfernungen verlangen, sondern es müssen auch die inhärenten Schwächen des Internets in Bezug auf die Wahrung der Privatsphäre der Teilnehmer und den sicheren Datentransfer berücksichtigt werden.

Nur bei der umfassenden Gewährung von Sicherheit und Privatsphäre für alle Beteiligten bei der Verwendung des Internets als Hauptkommunikationskanal wird es möglich sein, eine virtuelle Universität erfolgreich zu betreiben. Aus diesen Gründen kann eine virtuelle Universität nur dann erfolgreich sein, wenn sie folgende Voraussetzungen erfüllt:

- Vertraulichkeit: Durch die Verschlüsselung von Daten wird die Privatsphäre der Nachrichtenübermittlung gewahrt.
- Authentifikation: Der Absender der Nachricht wird eindeutig identifiziert, es wird ausgeschlossen, dass sich jemand eine falsche Identität zulegt oder sich als eine andere Person ausgibt.
- Integrität: Die versandte Nachricht erreicht unverändert den Adressaten.
- Unwiderrufbarkeit: Der Sender kann die Autorenschaft einer Nachricht, die er gesendet hat, im Nachhinein nicht abstreiten.

Alle diese Eigenschaften können durch den Aufbau einer Public-Key-Infrastructure (PKI), wie sie das Institut für Telematik anbietet, nachhaltig erreicht werden.

In unserem Modell einer virtuellen Universität, das auf den jahrelangen Erfahrungen des Instituts im Bereich der Zertifikatsverwaltung bei Banken beruht, wird, auf offenen Standards basierend, eine PKI mit folgenden Komponenten geschaffen:

- Ein sicheres *elektronisches Studienbuch* wird für jeden Studierenden eingerichtet und beinhaltet die relevanten persönlichen Informationen wie Name, Immatrikulationsdatum und auch die abgelegten Scheine und Prüfungen.
- Ein *Zertifikats-Server* gibt den Teilnehmern die Möglichkeit, Zertifikate für die Kommunikation zu beantragen und diese auf ihrem Rechner zu installieren. Dadurch wird bei Aufsuchen der virtuellen Universität im Netz die Eingabe von Passwörtern überflüssig.
- Ein Directory-Server verwaltet die Zertifikate der Studierenden und Lehrenden sowie der Verwaltungsmitarbeiter zentral und speichert sie für alle nachprüfbar ab.
- Ein *Zeitstempeldienst* verschafft die Möglichkeit, Dokumente mit einer Zeitmarke zu versehen („Abgabeschluss"). Dies ist für die Abgabe von Hausarbeiten und Diplomarbeiten unerlässlich.
- *SmartCards, Disketten* oder auch *Festplatten* können für die persönliche Sicherheits-umgebung zur Speicherung privater Schlüssel zur Aktivierung der Zertifikate benutzt werden.

Die Zertifikate der Teilnehmer und der virtuellen Universität sowie der Zeitstempeldienst können zu folgenden Aufgaben genutzt werden:

- Zugriff auf das elektronische Studienbuch
- Signieren von Scheinen und Prüfungsergebnissen
- Signieren und Verschlüsseln von E-Mails
- Erwerb von Studienunterlagen
- Antragstellung bei der Uni-Verwaltung
- Verschlüsselter Versand der Kreditkartennummer für Gebührenzahlung
- Versendung persönlicher privater Informationen zur Universitätsverwaltung
- Verteilung von Forschungsergebnissen
- Einsicht auf persönlichen Daten von Studenten durch berechtigte Personen
- Zeitstempel, um die Existenz elektronischer Dateien zu einen bestimmten Zeitpunkt zu dokumentieren
- Aufnahmeanträge in Kursen mit einer begrenzten Zahl von Studenten

Das Institut für Telematik - Garant für den Erfolg

Während bislang die Vermittlung der Lerninhalte im Vordergrund der Konzepte zur virtuellen Hochschule steht, bietet das Institut für Telematik ein umfassendes Infrastruktur-Modell zur Umsetzung dieser Ansätze, das den modernen Ansprüchen an die sichere und vertrauliche Kommunikation in offenen Datennetzen gerecht wird. Die u.a. im Bankenbereich bewiesene Kompetenz des Instituts bei der Schaffung und dem Betrieb einer PKI mit mehreren zehntausend Teilnehmern ist dabei ein Garant für den Erfolg dieses Modells.