HUMBOLDT-UNIVERSITÄT ZU BERLIN
COMPUTER-UND MEDIENSERVICE (RECHENZENTRUM)

„Sicher vernetzte Universitätsverwaltung und Dezentralisierung“

Abschlussbericht an den DFN-Verein

20. Oktober 2003

Auftragnehmer	Humboldt-Universität zu Berlin ZE Computer- und Medienservice (bis 31.12.2002 Rechenzentrum)
Kennzeichen	**TK 602-SD 113**
Kurzbezeichnung	UVsec
Laufzeit des Vorhabens	01.02.2000 – 31.05.2003
Berichtszeitraum	01.02.2000 – 31.05.2003
Projektleitung	Herr Dr. P. Schirmbacher
Fachliche Betreuung	Frau D. Natusch
Projektdurchführung	Herr M. Bell Herr R. Herbst Herr T. Hoke Herr M. Schwan

Inhaltsverzeichnis

0 Vorbemerkungen

Kern des Abschlussberichtes ist der durch das Projektteam erarbeitete DFN-Bericht:

Bausteine für eine sichere Hochschulverwaltung
- praktische Erfahrungen bei der Realisierung einer VPN-Lösung -

Dieser DFN-Bericht befindet sich derzeit im Druck, sein Entwurf ist dem Abschlussbericht als Anlage beigefügt.

Die Fülle der im Projektzeitraum bearbeiteten Aufgaben und die Vielzahl der für andere DFN-Einrichtungen interessanten Ergebnisse münden in diesen DFN-Bericht. Auf über 170 Seiten wird dargelegt, wie zentrale Datenbestände mit sensiblen Personen-, Haushalts- und Studierendendaten auf geschützte Weise von dezentralen Verwaltungsbereichen genutzt werden können. Das inhaltlich-organisatorische Herangehen, das insbesondere für Entscheidungsträger und DV-Manager von Interesse sein könnte, wird beschrieben. Es wird das für IPsec-Verbindungen erforderliche theoretische Rüstzeug vermittelt. Die konkrete praktische Umsetzung des dezentralen Zugriffes und die Einbindung von Zertifikaten in eine VPN-Lösung ist Gegenstand eines weiteren sehr ausführlichen Teiles. Der DFN-Bericht wendet sich ebenfalls wirtschaftlichen Fragestellungen zu, wie z. B. den personellen Aufwendungen für die Entwicklung, Betreuung und Weiterentwicklung einer VPN-Lösung.
Der DFN-Bericht ist als Praxisleitfaden gedacht. Die praktischen Erfahrungen und Ergebnisse der Projektarbeit sind in einer Form dargestellt, die eine umfassende Nachnutzung durch die DFN-Anwendereinrichtungen und darüber hinaus z. B. auch durch die Forschungs- und Entwicklungs- bzw. Wissenschaftseinrichtungen gestattet.

Der vorliegende Abschlussbericht schildert deshalb nur kurz den Inhalt und den Verlauf des Projektes und sollte in engem Zusammenhang zum DFN-Bericht gesehen werden. Die Projektergebnisse werden noch einmal überblicksartig vorgestellt und der Nutzen für die DFN-Anwenderschaft in Form einer Übersicht über die Veröffentlichungen und Veranstaltungen aufgelistet.

1 Anliegen des Projektes

Fokus des Projektes war die Ausweitung des Vernetzungs- und Sicherheitskonzeptes auf die Fakultätsverwaltungen unter vorrangiger Betrachtung der Schnittstellen zwischen zentraler und dezentraler Hochschulverwaltung.

Um diese Aufgabe zu erfüllen, wurden im Projektangebot mehrere Arbeitspakete formuliert, die im Einzelnen folgende Inhalte hatten:

1. Weiterentwicklung des Firewallkonzeptes unter dem Aspekt der definierten Öffnung gegenüber den dezentralen Verwaltungsbereichen und unter Beachtung der noch nicht genügend einbezogenen Spezifik von Non-TCP/IP-Protokollen

2. Analyse der Bedrohungen, die sich aus der Umgehung des Firewallsystems ergeben – Aufstellung und Durchführung von Gegenmaßnahmen

3. Erprobung des Einsatzes von Smartcards in der Verwaltung der Universität am Beispiel einer konkreten Verwaltungsanwendung

4. Erprobung des Einsatzes von kryptographischen Verfahren auf Netzwerk-Ebene

5. Entwicklung von Referenzlösungen des Einsatzes von kryptographischen Technologien für ausgewählte DV-Systeme der Universitätsverwaltung

6. Dokumentation – Veröffentlichung eines Leitfadens für ein sicheres Verwaltungsnetz in Form eines DFN-Berichts

Die Ergebnisse der Projektarbeit lassen sich am einfachsten durch einen Vergleich der Situation zu Projektbeginn (Anfang 2000) und dem jetzigen Stand (September 2003) dokumentieren. Am Beginn des Projektes gab es netztechnisch und auch inhaltlich-organisatorisch eine strenge Trennung zwischen der zentralen Universitätsverwaltung und den Verwaltungsbereichen in den Fakultäten bzw. auch den Bereichen außerhalb der Universität. Diese Grenze verschwimmt in zunehmendem Maße bzw. wird definiert für ausgewählte DV-Anwendungen geöffnet. Inzwischen benutzt die Universitätsverwaltung eine gesicherte Fernverbindung zu einem Application Service Provider, um die Personalbezüge der Universität berechnen zu lassen. Und immer mehr Fakultätsverwaltungen haben eine direkte Smartcard-basierte VPN-Verbindung zu den zentralen Prüfungs- bzw. Haushaltsdatenbeständen der Universität.

Zusätzlich zu diesen konkreten praktischen Ergebnissen ist in den zurückliegenden Jahren im Computer- und Medienservice (CMS) ein umfangreiches Know-how auf dem Gebiet der IT-Security aufgebaut worden, welches sich von der Netzwerk-Sicherheit bis zu PKI und Krypto-Hardware erstreckt, also das ganze Spektrum dieses sehr umfangreichen Gebietes abdeckt. Dieses Know-how wurde im Projektzeitraum sehr aktiv in die Diskussionsforen von Security-Konzepten und -Lösungsvorschlägen mit anderen Hochschuleinrichtungen eingebracht. So sind die Durchführung von Security-Workshops und die aktive Teilnahme an zahlreichen DFN-Veranstaltungen beredte Beispiele hierfür.
Das UVsec-Team wurde ebenfalls in konzeptionelle Arbeiten zur weiteren Absicherung des Universitätsnetzes einbezogen. So war es an der Konzipierung eines Firewall- und VPN-Konzeptes für das gesamte Universitätsnetz und auch an der Erarbeitung eines Pflichtenheftes zum Aufbau einer Public Key Infrastructure an der Humboldt-Universität beteiligt.

Das Wirksamwerden des Projektteams über die Projektgrenzen hinaus und die intensive Kooperation mit anderen Hochschulen waren wesentlich für das Erreichen der Projektziele. Mit dem im Projektzeitraum angesammelten Know-how und Hintergrundswissen war es möglich, eine VPN-Lösung für sensible Verwaltungsdaten zu entwickeln, in einem Pilotversuch zu erproben und den Übergang vom Pilot- in den Regelbetrieb zu wagen. Die hierbei gemachten Erfahrungen können wiederum den anderen DFN-Anwendern zur Verfügung gestellt werden. Der als Anlage beigefügte DFN-Bericht soll diesen Weg für andere nachvollziehbar dokumentieren.

2 Ergebnisse

2.1 Projektverlauf

Während des Projektverlaufes wurde der Stand der Arbeiten in mehreren Zwischenberichten dokumentiert und dem DFN-Verein gemeinsam mit teilweise sehr umfangreichen Anlagen zur Verfügung gestellt:

1. Zwischenbericht an den DFN-Verein (August 2000)
2. Zwischenbericht an den DFN-Verein (Januar 2001)
3. Zwischenbericht an den DFN-Verein (August 2001)
4. Zwischenbericht an den DFN-Verein (September 2002)

Der nun vorliegende Abschlussbericht soll zusammenfassend die Schwerpunkte der Ergebnisse der Zwischenberichte hervorheben. Im letzten Projektabschnitt erfolgte die Erstellung eines DFN-Berichtes (Arbeitspaket 6), welcher die Ergebnisse des bisherigen Projektverlaufes zusammenfasst und der deshalb hier besonders zur Lektüre empfohlen werden soll. Der DFN-Bericht kann nach Druck direkt vom DFN-Verein bezogen werden und wird auch als PDF-Version den Mitgliedseinrichtungen des Deutschen Forschungsnetzes zur Verfügung gestellt werden.

Aufgrund von sich zusätzlich ergebenden Anforderungen ist der zeitliche Verlauf des Projektes einer Reihe von Veränderungen unterworfen worden, die jeweils in enger Abstimmung mit dem DFN-Verein erfolgten.

2.2 Beschreibung der Arbeitspakete

2.2.1 Arbeitspaket 1: Weiterentwicklung des Firewall-Konzeptes

2.2.1.1 Zielstellung

- Weiterentwicklung des Firewall-Konzeptes unter dem Aspekt der definierten Öffnung gegenüber den dezentralen Verwaltungsbereichen und unter Beachtung der noch nicht genügend einbezogenen Spezifik von Non-TCP/IP-Protokollen

2.2.1.2 Ergebnisse

Die Einrichtung und der Betrieb des Firewall-Systems zwischen dem Netzwerk der Universitätsverwaltung (Verwaltungsnetz) und dem übrigen Netzwerk der Universität (HU-Backbone) hat sich gerade in der näheren Vergangenheit bewährt. Im Verlauf des Projektzeitraumes wurde das gesamte System kontinuierlich weiterentwickelt.

Abb. 1 stellt eine Moment-Aufnahme der Kommunikations-Beziehungen der Nutzer des Verwaltungsnetzes mit verschiedensten Außenstellen dar, aus der die Vielschichtigkeit der Verbindungen hervorgeht.

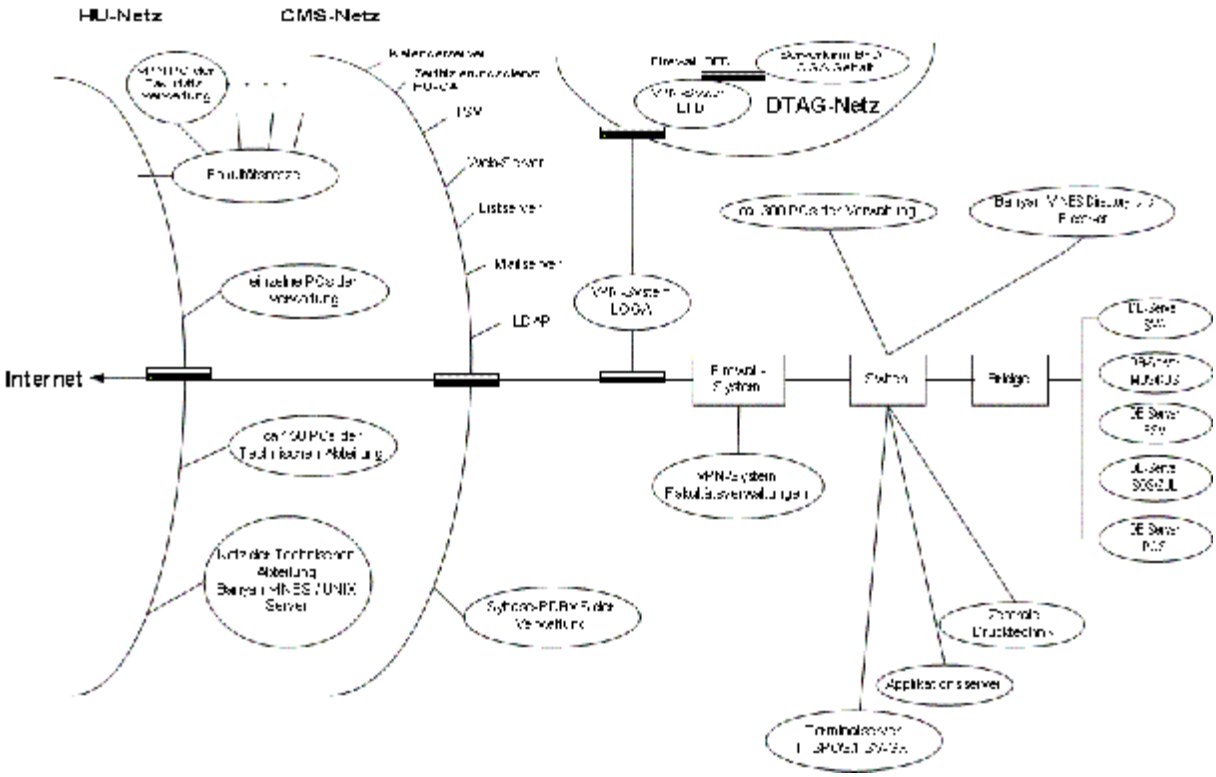

Abb.: 1 Universitätsverwaltung - Erreichter Stand der Vernetzung 9/2003

Aufgrund des vorliegenden Stufenkonzeptes konnten Angriffe aus dem Internet erfolgreich erkannt und verhindert werden. Die Informationen des Firewall-Log-Systems konnten gerade in der letzen Zeit zur Auswertung von Angriffen herangezogen werden, die in das HU-

Backbone zielten und so den Sensoren des Firewall-Systems der Universitätsverwaltung zugänglich wurden.
Durch die Kombination einer Standard-Client-Installation im Verwaltungsnetz mit Client-basiertem Virenscan mit automatischer Update-Funktion und dem Firewall-System war es möglich, die Verbreitung der netzwerkbasierten Viren (Ausnutzung von Schwachstellen der Implementierung des RPC-Protokolls in Win32-Systemen) innerhalb des geschützten Bereiches auf Null zu begrenzen.

Weitere Informationen zu Stand und Entwicklung des Firewall-Systems der Verwaltung („Das Firewall-System des Verwaltungsnetzes“) wurden im Heft 23 der RZ-Mitteilungen (s. Veröffentlichungen) publiziert, um die Ergebnisse auch anderen Forschungseinrichtungen und DFN-Mitgliedseinrichtungen zugänglich zu machen. Abgeschlossen wurde dieses Arbeitspaket mit der bereits erwähnten netztechnischen Anbindung an einen Application Service Provider (ASP). Über Terminalserver-Technologien sind die Mitarbeiter der Universitätsverwaltung mit dem Dienstleister verbunden. Das genaue Verfahren hierzu wurde auf dem öffentlichen Workshop „Sichere Netze – Beispiellösungen für die Universitätsverwaltung“ des UVsec-Projektes im Juli 2001 vorgestellt (s. Veranstaltungen).

2.2.2 Arbeitspaket 2: Zusätzliche Gefahren durch die Umgehung des Firewall-Systems

2.2.2.1 Zielstellung

- Der Schwerpunkt dieses Arbeitspaketes liegt auf der Erkennung und Klassifizierung von Gefahren im Rahmen unserer derzeitigen Netzwerkinfrastruktur. Bei der Analyse und Klassifizierung rücken zwei Punkte ins Zentrum unseres Interesses - die Entwicklung eines Konzeptes für die Sicherung und Archivierung von sensiblen Verwaltungsdaten außerhalb der Firewall und die Untersuchung von Netzwerkanalyse- und Managementtools.

2.2.2.2 Ergebnisse

Die Daten der UNIX-Server der Universitätsverwaltung werden über das zentrale Backup-System des CMS gesichert. Die Entwicklung, Erprobung und Einführung des Verfahrens geschah in enger Zusammenarbeit mit den Administratoren der jeweilig beteiligten Systeme. Das genaue Verfahren ist in einem Artikel eines der Administratoren des zentralen Backup- und Archivsystems der HU im Heft der RZ-Mitteilungen Heft 23 („Sicherung von Verwaltungsdaten“) veröffentlicht.

Im zweiten Teil dieses Arbeitspaketes wurde ein zentrales und verteiltes Intrusion Detection System (DIDS) implementiert. Das Ergebnis wurde auf dem Workshop im Juli 2001 (s. Veranstaltungen) vorgestellt. Teile unserer Ergebnisse der Entwicklung flossen direkt in den Quellcode der genutzten Open Source Projekte Snort und ACID ein (http://www.snort.org/ und http://www.cert.org/kb/acid/).

2.2.3 Arbeitspaket 3: Erprobung des Einsatzes von Smartcards in einer Universitätsverwaltung

2.2.3.1 Zielstellung

- Ziel dieses Arbeitspaketes ist die Einführung einer Public Key Infrastructure (PKI) der HU-Berlin, wobei die Unterstützung von Smartcards als Speicher des geheimen Schlüssels und/oder geheimen Signaturschlüssels untersucht werden soll.

2.2.3.2 Ergebnisse

Gemeinsam mit den Herstellern von Smartcards und Sicherheits-Token wurden die Möglichkeiten analysiert, diese Hardware aus Standard-E-Mail-Applikationen und Standard-Browsern heraus anzuwenden. Die Ergebnisse dieser Untersuchungen wurden u.a. auf DFN-Arbeitstagungen veröffentlicht und so einem breiteren Anwenderkreis zur Verfügung gestellt.

Einer der UVsec-Projektmitarbeiter ist mittlerweile im dritten Jahr im Core-Developer-Team des OpenCA-Projektes (`http://www.openca.org/`) tätig, einem Projekt, welches es sich zur Aufgabe gestellt hat, eine Open Source-basierende Public Key Infrastructure für die Allgemeinheit (also speziell für die Einrichtungen des öffentlichen Bereiches) zu entwickeln und kostenfrei zur Verfügung zu stellen. Nicht zuletzt dadurch wird es Universitäten und öffentlichen Einrichtungen erst möglich, Sicherheitslösungen auf hohem Niveau zu etablieren.

Aufgrund der Ablösung eines nicht-standard-basierten E-Mail-Systems mit einem SMTP-basierten System ergab sich die Anforderung, eine Verschlüsselungslösung für die Abteilung Personal und Personalentwicklung zu entwickeln. Besonderer Wert wurde dabei auf die Nutzung eines Open Source basierenden Systems gelegt, um die entstehenden Nachfolge-Kosten möglichst gering zu halten. Die Wahl fiel auf das OpenCA-System. Es wurde eine Komplett-Lösung implementiert, welche von den Anwendern sehr gut angenommen wurde und die bis zum jetzigen Zeitpunkt fehlerfrei funktioniert.

2.2.4 Arbeitspaket 4: Kryptographische Verfahren auf Netzwerk-Ebene

2.2.4.1 Zielstellung

- Ziel ist es, herauszufinden, inwiefern man die Sicherheit eines zu schützenden Bereiches durch den Einsatz von IPsec-Technologien erhöhen kann. Es ist zu erwarten, dass IPsec eine weite Verbreitung erfahren wird, da es Bestandteil der Netzwerkarchitektur von Windows2000 sein wird, welches aus gegenwärtiger Sicht das zukünftige Client-OS der Verwaltung darstellt.

2.2.4.2 Ergebnisse

Kryptographische Verfahren auf Netzwerkebene dienen nicht nur der Verschlüsselung von Daten, sondern sie gewährleisten auch die Authentizität des Kommunikationspartners. Getestet wurden hierzu die Produkte F-Secure VPN+ und die Implementierung des IPSec-Standards der Firma Microsoft innerhalb des Betriebssystems Windows 2000.

Im Mai 2002 erschien Heft 23 der RZ-Mitteilungen mit dem Thema „Computereinsatz in der Universitätsverwaltung“. In dem Artikel „Licht und Schatten am Ende des Tunnels“ wurden die Ergebnisse zusammenfassend beschrieben.

In detaillierter Form werden die Ergebnisse dieses Arbeitspaketes innerhalb des DFN-Berichtes „Bausteine für eine sichere Hochschulverwaltung“ in mehreren Kapiteln dargestellt. So werden z. B. verschiedene Konzepte für einen sicheren dezentralen Zugriff diskutiert und die Protokolle der IPSec-Familie ausführlich erklärt.

2.2.5 Arbeitspaket 5: Entwicklung von Referenzlösungen für ausgewählte DV-Systeme der Universitätsverwaltung

2.2.5.1 Zielstellung

- Im Rahmen dieses Arbeitspaketes sollen für schon existierende oder in der Einführung begriffene Systeme der Verwaltung Sicherheitslösungen geschaffen werden, die eine Nutzung der Software auch außerhalb der Firewall sicher macht.

2.2.5.2 Ergebnisse

Mittels des Produktes F-Secure VPN+ wurde eine nachnutzbare Referenzlösung geschaffen, um die sichere Anbindung von dezentralen Bereichen der Universitätsverwaltung zu realisieren. Alle Arbeitspakete des UVsec-Projektes werden davon berührt. Die Lösung wurde über mehrere Stufen (Machbarkeit, Pilot, Produktion) in die Routine übernommen. Zum Einsatz für Authentifizierung und Verschlüsselung kommen dabei von der HU-CA via OpenCA erstellte Zertifikate, die sich auf Smartcards befinden. Die dezentralen Nutzer arbeiten über Terminalserver-Technologie direkt auf den zentralen DBMS-Systemen der Universitätsverwaltung. Auch hier sei ergänzend auf die Lektüre der umfangreichen Anlage verwiesen.

2.2.6 Arbeitspaket 6: Dokumentation zur Nachnutzung durch andere Hochschulverwaltungen

2.2.6.1 Zielstellung

- Ziel dieses Arbeitspaketes ist es, die einzelnen Teilergebnisse zusammenzufassen und für Dritte nachnutzbar zu gestalten. Hier soll der Versuch unternommen werden, einen Leitfaden in der Form eines DFN-Berichtes zu schreiben, welcher einen hohen Nachnutzbarkeitswert besitzt.

2.2.6.2 Ergebnisse

Das Ergebnis dieses Arbeitspaketes ist der DFN-Bericht „Bausteine für eine sichere Hochschulverwaltung“ - Praktische Erfahrungen bei der Realisierung einer VPN-Lösung, der als Anlage beigefügt ist.

3 Öffentlichkeitsarbeit

Innerhalb des UVsec-Projektes wurden die Ergebnisse der Forschungs- und Entwicklungstätigkeit fortlaufend auf verschiedenen Wegen publiziert und somit auch anderen DFN-Mitgliedseinrichtungen zugänglich gemacht. So wurde vom Projektteam im Juli 2001 ein öffentlicher Workshop mit dem Titel „Sichere Netze – Beispiellösungen für die Universitätsverwaltung“ organisiert und durchgeführt, der mit Gästen aus ganz Deutschland stattfand.
Nachfolgend werden die im Projektzeitraum durchgeführten Öffentlichkeitsarbeiten, gegliedert nach Veröffentlichungen, Veranstaltungen und Vorträgen sowie internationalen Projekten, chronologisch zusammengefasst.

3.1 Veröffentlichungen

- DFN-Mitteilungen Heft 56 / Juni 2001: „Sicherheit in Verteilten Netzen“
- RZ-Mitteilungen Nr. 22 / November 2001: „Sicher vernetzte Universitätsverwaltung und Dezentralisierung (UVsec)“
- RZ-Mitteilungen Nr. 23 / Mai 2002: „Das Firewall-System des Verwaltungsnetzes“
- RZ-Mitteilungen Nr. 23 / Mai 2002: „Verschlüsseln und Signieren von E-Mails - eine einfache Anwendung?“
- iX 6/2002, Seite 139: „Verlegt - Private Keys vor Zugriff schützen“
- RZ-Mitteilungen Nr. 23 / Mai 2002: „Licht und Schatten am Ende des Tunnels“
- CMS-Journal Nr. 24 / April 2003: „Public Key Infrastructure - ein Blick in die nahe Zukunft“
- noch nicht erschienen, aber als Anlage beigefügt:

DFN-Bericht „Bausteine für eine sichere Hochschulverwaltung“
- Praktische Erfahrungen bei der Realisierung einer VPN-Lösung -

3.2 Veranstaltungen und Vorträge

- „Die Digitale Signatur“ auf einer RZ-internen Veranstaltung am 5. September 2000
- „Aufbau und Funktionsweise einer PKI“ auf einem RZ-Kolloquium am 21. November 2000
- „PKI-enabled Applications“ auf einem RZ-Kolloquium am 21. November 2000
- „OpenSSL und Smartcards ?“ auf der DFN-Betriebstagung am 6. Februar 2001
- „Aufbau einer Sicherheitsinfrastruktur an der HU Berlin“ auf der 5. Tagung der DFN-Nutzergruppe Hochschulverwaltung vom 19. Februar bis 21. Februar 2001 in Kassel
- „Streaming und Firewall ?“ auf dem 3. Workshop des BZVD am 12. März 2001 in Dresden
- Security-Workshop „Sichere Netze – Beispiellösungen für die Universitätsverwaltung“ am 9. Juli 2001 im Senatssaal der Humboldt-Universität zu Berlin
  - „Ziele und Motivation des Projektes Sicher vernetzte Universitätsverwaltung und Dezentralisierung (UVsec)“
  - „Die elektronische Signatur - Voraussetzungen und Anwendungsmöglichkeiten“
  - „Möglichkeiten und Grenzen des Aufbaus eines Trustcenters an Hochschulen“
  - „Dezentraler Zugriff auf zentrale Daten über geschützte Netze“
  - „Application Service Provider (ASP) - Einsatz von Terminalserver-Clients hinter einem Firewallsystem“

  - „Netzwerküberwachung mit Hilfe von Distributed Intrusion Detection Systems (DIDS)“
- „Dezentraler Zugriff auf zentrale Daten über geschützte Netze“, Vortrag auf der Sitzung der DFN-Nutzergruppe Hochschulverwaltung am 11.10.2001 in Berlin
- „Thin Clients und Smartcards an der HU“ auf der Tagung 2003 der DFN-Nutzergruppe Hochschulverwaltung "Verwaltung@eUniversity" 15. - 17. Mai 2003 in Potsdam

3.3 Internationale Projekte

- Mitarbeit im Core-Developer-Team des OpenCA-Projektes (http://www.openca.org/)

Anlage 1

DFN-Bericht „Bausteine für eine sichere Hochschulverwaltung“ - Praktische Erfahrungen bei der Realisierung einer VPN-Lösung