



## Aufgabenstellung für die Diplomarbeit von

Herrn : Jan Tobias Mühlberg  
Matrikelnummer : 992024  
Studiengang : Informatik  
Studienrichtung : Intelligente Systeme

Thema : „Konzeption und prototypische Umsetzung von Authentifizierungsverfahren und Kommunikationsschnittstellen für das Identity Management System CIDAS unter besonderer Berücksichtigung mobiler identifizierbarer Datenträger“

**Aufgabenstellung:** In der von Herrn Mühlberg zu schreibenden Diplomarbeit soll vorrangig ein auf der Verwendung mobiler identifizierbarer Speichermedien und asymmetrischer Kryptographie basierendes Authentifizierungsverfahren zum Einsatz im an der Fachhochschule Brandenburg entwickelten Identity Management System CIDAS (Configurable Internet Directory and Authentication Service) konzipiert werden. Darüber hinaus soll ein für die sichere Kommunikation zwischen Authentifizierungsserver und -client geeignetes Kommunikationsprotokoll unter Berücksichtigung der Besonderheiten des Systems CIDAS entworfen werden. Die Ergebnisse der konzeptionellen Tätigkeit sind prototypisch umzusetzen und zu präsentieren.

**Schwerpunkte:** Herr Mühlberg soll sich insbesondere mit

- Verfahren zur Benutzerauthentifizierung auf Basis asymmetrischer Kryptographie,
- der Identifizierung von Datenträgern, insbes. USB-Memory-Sticks, CD-ROMs und RFIDs (kontaktlose Transponder) und
- dem Entwurf sicherer Kommunikationsprotokolle

befassen.

Betreuer : Prof. Dr. Friedrich-L. Holl, FH Brandenburg  
1. Prüfer : Prof. Dr. Friedrich-L. Holl, FH Brandenburg  
2. Prüfer : Prof. Dr. Barbara Wiesner, FH Brandenburg  
Ausgabe der Aufgabenstellung : 03. November 2003  
Abgabe der Diplomarbeit bis zum : 20. Februar 2004