

# Jahresbericht 2006

## Zusammenfassender Bericht über die Aktivitäten der Stiftung Secure Information and Communication Technologies SIC

Die Stiftung Secure Information and Communication Technologies SIC wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) als gemeinnützige Stiftung gegründet und mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 für zulässig erklärt. In diesem Jahresbericht werden die Aktivitäten der Stiftung im Geschäftsjahr 2006 berichtet.

## Inhaltsverzeichnis

Inhaltsverzeichnis	1
Executive Summary	2
1 Einleitung	3
1.1 Stiftungszweck	3
1.2 Forschungsschwerpunkte	3
1.3 Zur Lage der Stiftung	4
1.4 Hilfsbetrieb JCE Toolkit	4
1.5 Stiftungsorgane und Organisationsstruktur	5
2 Leistungen im Sinne des Stiftungszwecks	7
2.1 Förderung von Forschung und Lehre, Wissenstransfer	7
2.1.1 Stiftungsprofessur Informationssicherheit	7
2.1.2 Vorlesung Kritische Informationsinfrastrukturen	8
2.1.3 RFID-Initiative PROACT	8
2.1.4 E-Government	9
2.2 Eigenständige Forschung und Entwicklung	9
2.2.1 Forschungsprojekt POSITIF	9
2.3 Organisatorisches und Sonstiges	9
2.3.1 Technische Infrastruktur	10
2.3.2 Entwicklungsaktivitäten JCE Toolkit	10
Anhang: Pressemeldungen	11

### Auskünfte

Stiftung Secure Information and Communication Technologies SIC  
Inffeldgasse 16a  
8010 Graz  
Tel.: (0316) 873-5513 / 5521 Fax.: (0316) 873-5520

### Impressum

Medieninhaber, Herausgeber und Verleger

Stiftung Secure Information and Communication Technologies SIC, Inffeldgasse 16a, 8010 Graz

Redaktion und für den Inhalt verantwortlich

Dipl.-Ing. Herbert Leitold, Dr. Peter Lipp (Vorstand der Stiftung)

Graz, am 20. Juni 2007



## Executive Summary

Die Stiftung Secure Information and Communication Technologies SIC wurde im Februar 2003 gegründet und mit einem Stammvermögen von € 2.320.000 ausgestattet. Der Zweck der Stiftung ist *„die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit“*. Satzungsgemäß kann dies durch *„... Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen ...“* erfolgen.

Dieser Jahresbericht 2006 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1.2006 – 31.12.2006 dar. In diesem Zeitraum konnte die Stiftung in allen Bereichen des Stiftungszwecks wertvolle Beiträge leisten:

- Seitens der TU-Graz wurde 2006 die *„Stiftungsprofessur Informationssicherheit“*, die von der Stiftung SIC initiiert wurde, in eine permanente Professur übergeführt. Die Stiftung hat hier die zu Beginn 2004 ursprünglich auf fünf Jahre gegebene Finanzierungszusage auf zuerst eine volle Finanzierung und dann eine Teilfinanzierung bis 2012 erweitert. Dies stärkt die Forschung und Lehre in der Steiermark im Bereich des Stiftungszwecks.
- Aus dem Bereich Lehre wurde des Weiteren eine Lehrveranstaltung *„Kritische Informationsinfrastrukturen“* an der TU Graz finanziert. Dieses zunehmend wichtiger werdende Thema wurde Studierenden damit erstmals in einer eigenen Vorlesung vermittelt.
- Die bereits 2005 mit der Firma NXP (vormals Philips) gestartete Initiative *„Programme for Advanced Contactless Technology“* (PROACT) wurde fortgeführt. Unter anderem wurden Diplomarbeiten betreut, Forschung finanziert, bzw. in einer Summer School das Thema Radio Frequency Identification (RFID) an Studierende vermittelt.
- Im Bereich E-Government hat sich die Stiftung zusammen mit der TU Graz an Projekten des Landes Steiermark und des Bundes beteiligt.
- Das von der EU geförderte Projekt POSITIF zu Intrusion Detection, an dem die Stiftung beteiligt ist, wurde im seinem dritten Projektjahr im Wesentlichen abgeschlossen. Es handelt sich dabei um eigenständige Forschung der Stiftung.

Das Dokument stellt den nach dem Steiermärkischen Stiftungs- und Fondsgesetz an die Stiftungsbehörde als staatliche Aufsicht über die Stiftung zu übermittelnden Bericht dar.

In dieser im Internet veröffentlichten Version des Jahresberichts werden im Gegensatz zum Bericht an die Stiftungsbehörde die Details zur finanziellen Lage der Stiftung nicht wiedergegeben.



# 1 Einleitung

Die „Stiftung Secure Information and Communication Technologies SIC“ – in diesem Bericht in Folge als „die Stiftung“ bezeichnet – wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) im Jahr 2003 gegründet. Rechtliche Grundlage ist das *Steiermärkische Stiftungs- und Fondsgesetz, LGBl. Nr. 69/1988* – in Folge als *StSFG* abgekürzt. Mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 wurde die Stiftung für zulässig erklärt. In diesem Jahresbericht wird die Tätigkeit der Stiftung im Jahr 2006 dargestellt. Es stellt dies auch den Bericht über die im Sinne des Stiftungszwecks erbrachten Leistungen gemäß *StSFG § 14 (3)* dar (Abschnitt 2 „Leistungen im Sinne des Stiftungszwecks“). In den Anhängen sind die weiteren nach *StSFG § 14 (3)* definierten Berichte an die Aufsichtsbehörde angefügt.

Entsprechend einem Beschluss des Kuratoriums der Stiftung vom 8. Mai 2007 ist dieser Bericht im Internet zu veröffentlichen (ohne Finanzdaten, Bilanz und Rechnungsabschluss).

In diesem einleitenden Abschnitt werden die Grundlagen der Stiftung zusammengefasst.

## 1.1 Stiftungszweck

Der gemeinnützige Stiftungszweck ist in Artikel III. der Satzung wie folgt definiert:

*Zweck der Stiftung ist die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit durch Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen, die zur Erreichung des Stiftungszweckes beitragen. Diese stellen den begünstigten Personenkreis gemäß § 10 Abs. 2 Z 3 des Steiermärkischen Stiftungs- und Fondsgesetzes dar.*

*Die Leistungen der Stiftung erfolgen aus den Erträgen des Stiftungsvermögens bzw. aus dem Stiftungsvermögen selbst. Sämtliche Leistungen der Stiftung sind freiwillig und begründen keinen Rechtsanspruch gegen die Stiftung. Über die Gewährung von Leistungen der Stiftung entscheiden die Organe der Stiftung.*

Die gesamte Satzung ist in der Willbriefsammlung des Steiermärkischen Landesarchivs unter LReg. Vertrag Nr. 5509 hinterlegt bzw. auch im Internet unter der Adresse [http://sic.iaik.tugraz.at/sic/about\\_us/stiftung/satzung](http://sic.iaik.tugraz.at/sic/about_us/stiftung/satzung) veröffentlicht.

## 1.2 Forschungsschwerpunkte

Die allgemeine Formulierung des Stiftungszwecks soll dem in der Informationsverarbeitung, der Kommunikationstechnologie und der Informationssicherheit immens schnelllebigen technologischen Fortschritt begegnen, wo einzelne Forschungsgebiete sich laufend wandeln, jedoch in der auf Dauer eingerichteten Stiftung auf lange Sicht ein entsprechend vitales Betätigungsfeld anzunehmen ist.



Um die Leistungen der Stiftung dennoch der aktuellen technologischen und wissenschaftlichen Situation angepasst gestalten zu können, wurden aktuelle Schwerpunkte definiert.

Als aktuelle Forschungsschwerpunkte sind festgelegt:

- Sicherheitsaspekte der Informationsgesellschaft, insbesondere E-Commerce und E-Government
- Kryptographie und Kryptoanalyse
- Hardware- und Software-Umsetzung kryptographischer Verfahren
- Public Key Infrastrukturen und elektronische Signaturen
- Netzwerksicherheit
- Radio Frequency Identification - RFID
- Beiträge zur Standardisierung in obgenannten Bereichen

Diese Forschungsschwerpunkte schließen andere, im Rahmen des Stiftungszwecks rechtfertigbare Leistungen nicht aus, sondern geben eine grobe Richtlinie zu besonders förderungswürdigen Themen. Die Schwerpunkte sollen auch laufend an aktuelle Gegebenheiten angepasst werden.

### **1.3 Zur Lage der Stiftung**

In den bisherigen etwas über drei Jahren ihres Bestehens ist es der Stiftung gelungen, über Forschungsförderungen, Zuwendungen, Kooperationen und Gewinne des Hilfsbetriebs Toolkit Leistungen in einem Ausmaß zu erbringen, die deutlich über den reinen Ertrag des Stammvermögens hinausgehen. Es konnten Rücklagen gebildet werden, die auch in absehbarer Zukunft einen kontinuierlichen Betrieb der Leistungen am derzeit quantitativ und qualitativ hohen Niveau oder auch Investitionen in neue Forschungsgebiete erlauben, ohne noch auf das Stammvermögen zurückgreifen zu müssen.

Im Berichtszeitraum 2006 wurde im Bereich der gemeinnützigen Leistungen der Stiftung wieder eine Reihe von Aktivitäten finanziert. Leistungen aus dem Stiftungszweck mit Impulsen in der Ausbildung der Studierenden an der TU Graz waren vor allem die Stiftungsprofessur Kryptographie und die Vorlesung zu kritischen Informationsinfrastrukturen. Damit wurde der Ausbau der Kryptographie in Graz unterstützt bzw. ein neuer Bereich erschlossen. In der eigenständigen Forschung wurde das EU Forschungsprojekt POSITIF inhaltlich weitestgehend abgeschlossen.

Extern finanziert ist die Initiative PROACT in der die Stiftung die von NXP gestellten Mittel treuhändisch verwaltet. Weiters tragen Mitarbeiter der Stiftung gegen Kostenersatz zu E-Government Projekten des Landes Steiermark und des Bundes bei.

Der Hilfsbetrieb „JCE Toolkit“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Angesichts des geringen Personalstands in der Stiftung selbst wurden wissenschaftliche Weiterentwicklungen und notwendige Support- und Wartungsaufgaben an die TU Graz vergeben.

### **1.4 Hilfsbetrieb JCE Toolkit**

Mit Übertragung des „JCE Toolkit“ durch das IAIK Ende 2003 besteht ein Hilfsbetrieb, über den die Stiftung Zuflüsse über die Erträge aus dem pekuniären Stammvermögen bzw. aus der Veranlagung der Rücklagen hinausgehend erzielen kann.



Mit Bescheid der Finanzlandesdirektion aus 2003 wurde festgestellt, dass der Vertrieb des JCE Toolkit keine Begünstigung auf abgaberechtlichem Gebiet zukommt, jedoch die Begünstigung in den gemeinnützigen Bereichen weiterhin erhalten bleibt. Es wurde hier die Auflage erteilt, die Gewinne aus der kommerziellen Verwertung den gemeinnützigen Aktivitäten zuzuführen. Diese auch im Übertragungsvertrag des IAIK gegebene Maßgabe wurde bereits 2004 in der Satzung verankert.

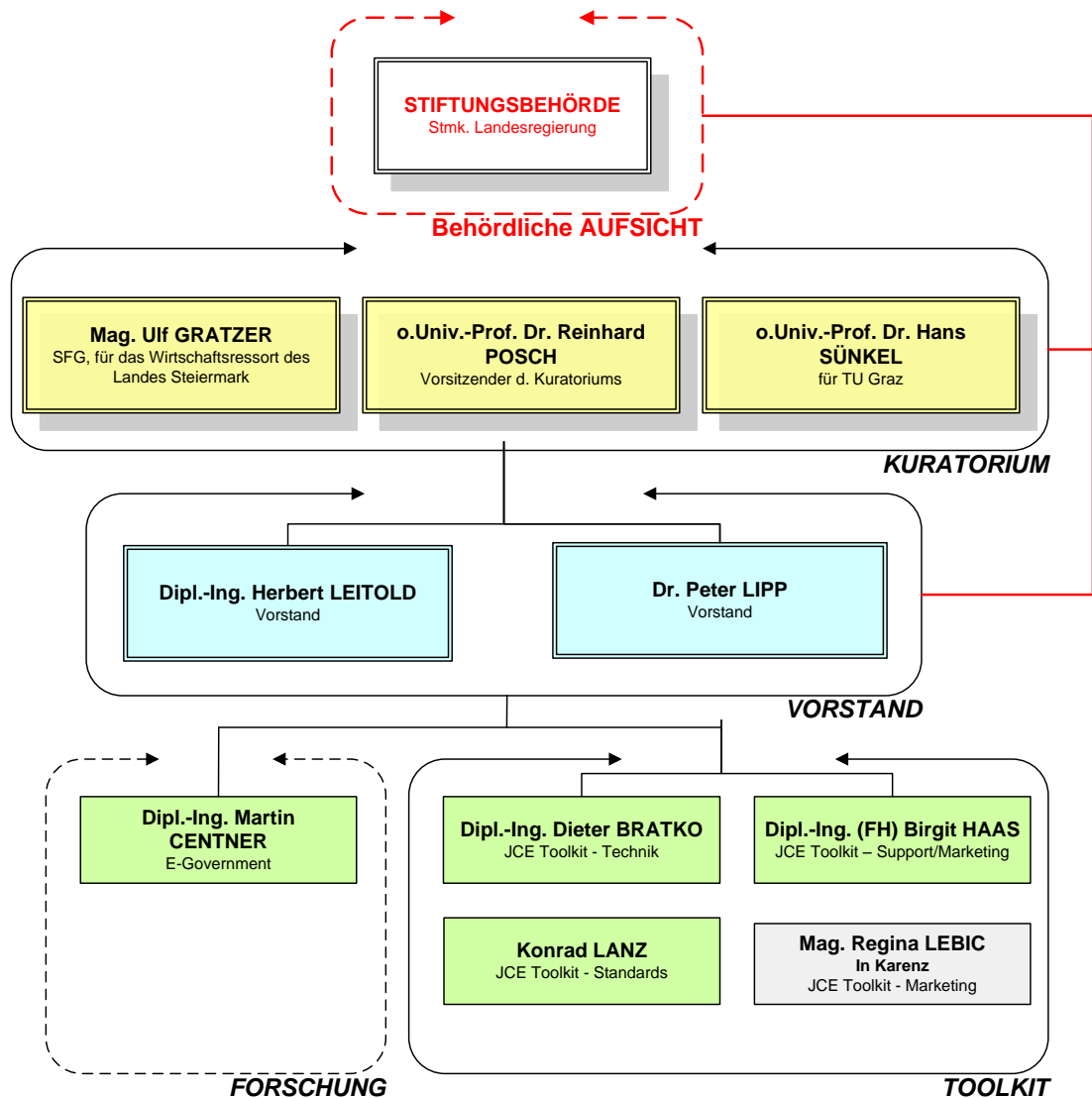
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden). Zusätzlich wurde 2005 der Bereich „PROACT“ angelegt, um die Gebarung dieser gemeinnützigen Aktivität gegenüber den industriellen Kooperationspartnern gesondert dokumentieren zu können.

## **1.5 Stiftungsorgane und Organisationsstruktur**

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2006 waren dies:
    - Mag. Ulf Gratzner (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
    - o.Univ.-Prof. Dr. Hans Sünkel (für die TU Graz)
  - Staatliche Aufsicht ist die Stiftungsbehörde FA7C der Steiermärkischen Landesregierung
- Die Führungsebene bildet der Vorstand
  - Dipl.-Ing. Herbert Leitold
  - Dr. Peter Lipp
- Die operative Ebene wird durch zwei Säulen gebildet:
  - Der Bereich *Forschung* umfasst die mit eigenständiger Durchführung von Forschung und Entwicklung befassten MitarbeiterInnen der Stiftung.
  - Der Bereich *Toolkit* ist als Hilfsbetrieb vom gemeinnützigen Bereich *Forschung* abgegrenzt, unterstützt diesen jedoch über Gewinne und in der nicht-kommerziellen Forschung kostenlos verwendbare Werkzeuge.

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Stand an Mitarbeiterinnen und Mitarbeitern der Stiftung per 31.12.2006 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2006.

## 2 Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird dem in der Satzung der Stiftung definierten *Stiftungszweck* entsprechend in „*Förderung von Forschung und Lehre*“ und „*Eigenständige Forschung und Entwicklung*“ strukturiert berichtet.

### 2.1 Förderung von Forschung und Lehre, Wissenstransfer

#### 2.1.1 Stiftungsprofessur Informationssicherheit

Seit 1.10.2004 ist die Stiftungsprofessur Informationssicherheit mit Prof. Dr. Vincent Rijmen besetzt. Dabei finanziert die Stiftung die Personalkosten von Prof. Rijmen, die TU Graz stattet die Stiftungsprofessur mit Räumlichkeiten, Assistenten und Sekretariat aus.

2006 wurde diese Stiftungsprofessur an der TU Graz permanent eingerichtet. Die Stiftung hat dazu die Finanzierungszusage zeitlich und im Umfang bis 2012 verlängert.

Die Gruppe um Prof. Rijmen konnte 2006 zahlreiche wissenschaftliche Publikationen veröffentlichen:

1. Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen: „*Analysis of Step-Reduced SHA-256*“ Fast Software Encryption - FSE 2006, Graz, Austria, March 15-17, 2006.
2. Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen: „*The Impact of Carries on the Complexity of Collision Attacks on SHA-1*“ Fast Software Encryption - FSE 2006, Graz, Austria, March 15-17, 2006.
3. Norbert Pramstaller, Christian Rechberger, Vincent Rijmen: „*A Compact FPGA Implementation of the Hash Function Whirlpool*“ 14<sup>th</sup> ACM/SIGDA International Symposium on Field-Programmable Gate Arrays - FPGA 2006, Hyatt Regency Monterey, Monterey, California, February 22-24, 2006.
4. Christophe De Canniere, Christian Rechberger: „*Finding SHA-1 Characteristics*“ Asiacrypt, Shanghai, December 3-7, 2006.
5. Martin Feldhofer, Christian Rechberger: „*A Case Against Currently Used Hash Functions in RFID Protocols*“ First International Workshop on Information Security (IS'06), LNCS Vol. 4277, Montpellier, France, Oct 30 - Nov 1, 2006.

Dabei besonders hervorzuheben ist die Veröffentlichung bei Asiacrypt (Nummer 4. In obiger Liste). Asiacrypt zählt zu den namhaftesten Konferenzen in der Kryptographie. Aus über 300 Einreichungen wurden 30 für den Tagungsband ausgewählt und daraus hat das Papier von Rechberger und De Canniere den Best Paper Award erhalten.

Ein weiteres Highlight in der Forschung sind signifikante Verbesserungen in den Methoden zum Finden von Kollisionen zur Hash-Funktion SHA-1. SHA-1 ist derzeit die gebräuchlichste Hash-Funktion bei sicheren elektronischen Signaturen. Die Arbeiten zu Angriffen lassen den aktuellen Sicherheitswert besser einschätzen. Die Gruppe um Prof. Rijmen konnte die Methoden zur Kollisionsfindung so verallgemeinern bzw. Algorithmen so verbessern, dass bei reduziertem SHA-1 mit 64 (der sonst 80) Berechnungsrunden eine Kollision gefunden werden konnte. Dies sind die weltweit derzeit besten bekannten Ergebnisse zu Angriffen auf SHA-1. Die Methoden sind hier bereits so ausgegriff, dass



diese Ergebnisse mit Rechenkapazität von handelsüblichen PCs möglich sind. Dabei wurden auch Methoden zu „teilweise sinnvollen Kollisionen“ entwickelt. Diese Ergebnisse erringen internationale Beachtung.

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „Angewandte Kryptographie“ und „Angewandte Kryptographie 2“, „Einführung in die Informationssicherheit“ und „IT-Sicherheit“ betreut. Das Angebot wird mit Seminaren, Projekten und Diplomarbeiten ergänzt.

Mit der Einrichtung der Stiftungsprofessur konnte also schon in der relativ kurzen Zeit seit 2004 Graz und die TU zu einem international beachteten Zentrum in der Kryptographieforschung entwickelt werden.

### **2.1.2 Vorlesung Kritische Informationsinfrastrukturen**

Mit der zunehmenden Abhängigkeit der Gesellschaft von Informationstechnologie entwickeln sich viele Informations- und Kommunikationssysteme zur kritischen Infrastruktur. Durch die zunehmenden Abhängigkeiten der kritischen Infrastrukturen wie Energieversorgung, Verkehr oder Telekommunikation voneinander ist deren Schutz ein immer komplexer werdendes Problem. Funktionsstörungen etwa als Folge von Naturkatastrophen, Angriffen oder Systemfehlern können bereits heute die Wirtschaft schwer schädigen oder das öffentliche Leben beträchtlich stören.

Um solchen Szenarien vorzubeugen ist es wichtig, Konzepte und Methoden zum Schutz kritischer Informationsinfrastrukturen bereits in der Ingenieurausbildung zu vermitteln. Es ist dazu gelungen, Dr. Otto Hellwig für eine Vorlesung „*Kritische Informationsinfrastrukturen*“ an der TU Graz zu gewinnen. Dr. Hellwig war unter anderem Chief Information Officer des Bundeskanzleramts.

Die Vorlesung Kritische Informationsinfrastrukturen wurde im Wintersemester 2006/2007 gestartet. Die Kosten werden von der Stiftung SIC getragen.

### **2.1.3 RFID-Initiative PROACT**

Die bereits 2005 gestartete Kooperation mit NXP (vormals Philips) und der TU Graz „*Programme for Advanced Contactless Technology*“ (PROACT) hat 2006 den operativen Betrieb aufgenommen. Dabei verwaltet die Stiftung die von NXP als Industriepartner gestellten Mittel, über die dann nach Vorgaben eines Koordinierungskomitees, in dem die Stiftung Sitz und Stimme hat, Forschung und Lehre der RFID Technologie an der TU Graz finanziert werden.

In 2006 wurden dabei unter Anderem folgende Aktivitäten ausgeführt:

- Eine Sommerschule vom 10.-12. Juli 2006, an der über 50 Studierende teilnahmen. (siehe auch Pressemeldungen in Anhang: Pressemeldungen)
- Im Anschluss an die Sommerschule fand vom 12.-14. Juli 2006 ein internationaler Workshop RFID Security mit etwa 80 Teilnehmern statt.
- Eine Core Group RFID Security wurde am IAIK der TU Graz eingerichtet, die sich mit RFID-optimierten Hardware-Umsetzungen von Hash-Funktionen befasst.





- Ein Best-Paper Award wurde ausgeschrieben. Forscher und Studierende auf Magister- und Bakkelaureatebene sollten wissenschaftliche Artikel zum Thema RFID einreichen. Eine Jury reichte die Beiträge und es wurden eine Konferenzreise, Pocket-PCs, MP3-Player und USB-Sticks als Preise vergeben.
- In der Lehre wurde RFID in einigen Lehrveranstaltungen integriert. Weiters wurden über PROACT an der TU Graz neben einigen Studentenprojekten 2006 drei Diplomarbeiten zu RFID erfolgreich abgeschlossen und fünf weitere Diplomarbeiten gestartet.

### **2.1.4 E-Government**

Die Stiftung hat zusammen mit der TU Graz 2005 den Zuschlag einer Ausschreibung des Landes Steiermark zu Wissenstransfer und Koordination zu E-Government erhalten<sup>1</sup>. Diese Aktivität ist 2006 gestartet. Es werden hier bis 2010 zusammen mit der TU Graz durchgehend etwa ½ Person für E-Government Aktivitäten des Landes Steiermark gestellt.

Darüber unterstützen Mitarbeiter des Bereichs Forschung der Stiftung das E-Government Innovationszentrum, eine Initiative der TU Graz und des Bundeskanzleramts.

## **2.2 Eigenständige Forschung und Entwicklung**

### **2.2.1 Forschungsprojekt POSITIF**

Die Stiftung hat im 6. EU Rahmenprogramm im Forschungsprojekt „*Policy-based Security Tool and Framework (POSITIF)*“ teilgenommen. 2006 war das dritte Jahr des Projekts in dem die Stiftung die ihr zugeordneten Arbeitspakete abschließen konnte. Es waren deshalb ab Mitte des Jahres die mit dem Projekt befassten Mitarbeiter nicht mehr im Projekt notwendig und wurden vom IAIK der TU Graz für andere Projekte übernommen.

Aus dem Projekt bzw. auch inhaltlich verwandten Aktivitäten zu Intrusion Detection entstanden 2006 folgende wissenschaftliche Publikationen:

1. Günter Lackner, Mario Lamberger, Udo Payer, Peter Teufl: "*WiFi Chipset Fingerprinting*" DACH Mobility, Munich, Germany, October 17-18, 2006.
2. Stefan Kraxberger, Udo Payer: "*SOM-Based Lightweight Policy Verification*" TERENA 2006 Networking Conference, Catania (Sicily), Italy, May 15-18, 2006.

## **2.3 Organisatorisches und Sonstiges**

In diesem Abschnitt werden Aktivitäten berichtet, die zwar nicht in ursächlichem Zusammenhang mit dem gemeinnützigen Stiftungszweck stehen, jedoch als Hilfsbetrieb den gemeinnützigen Bereich fördern, oder als administrative und organisatorische Infrastruktur erforderlich sind, um die Stiftungsaktivitäten effizient durchzuführen.

---

<sup>1</sup> Teil 1 der Ausschreibung „GZ FA1B B1.40-5688/2005 Ressourcen für die Konzeption und Umsetzung von E-Government“



### **2.3.1 Technische Infrastruktur**

Die technischen Anlagen der Stiftung, wie PCs, wurden nur in geringem Maße ausgebaut. Die technische Infrastruktur der Stiftung wurde weiterhin vor allem vom IAIK der TU Graz getragen. Darüber hinausgehend wurde keine Infrastruktur angeschafft, da hier die qualitativ hochwertigen Ressourcen der TU Graz und des IAIK die Anschaffung eigener teurer Anlagen nicht rechtfertigt. Die Nutzung der Infrastruktur wird an das IAIK abgegolten.

### **2.3.2 Entwicklungsaktivitäten JCE Toolkit**

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb haben sich nach einem etwas schlechteren Jahr 2005 im Geschäftsjahr 2006 wieder entsprechend den Erwartungen entwickelt. Trotzdem wurde die vorsichtige Personalpolitik mit aus 2005 reduziertem Personalstand beibehalten, in der das Personal der Stiftung vor allem das Management, das Marketing und nur teilweise die technische Wartung und Weiterentwicklung übernimmt. Weitere wissenschaftliche Weiterentwicklungen und teilweise auch erforderlicher Support und Wartung wurden an das IAIK der TU Graz vergeben. Diese notwendigen Weiterentwicklungen konnten so flexibler an die Verkaufslage angepasst beauftragt werden, als dies mit Fixpersonal der Stiftung möglich ist.

Zur Erschließung neuer Geschäftsfelder wurde eine Common Criteria Zertifizierung des Produktes gestartet, die voraussichtlich im Juni 2007 abgeschlossen werden wird. Damit soll die Qualität des Produkts bescheinigt werden. In einigen sicherheitskritischen Anwendungen werden solche Zertifikate von den Produzenten gefordert.

# Anhang: Pressemeldungen

Zur RFID Sommerschule wurde in Online-Medien (Computerwelt, APA-IT) bzw. im Karriere-Standard berichtet.

Der Standard

Computerwelt



The screenshot shows an article from 'Enterprise Infrastruktur & Business-Software' dated 4/7/2006. The title is '.02 RFID Sonderausbildung in Graz'. The article discusses the RFID Summer School at TU Graz, mentioning that it is a highly sought-after event for students interested in RFID technology. It notes that the school is organized by Philips and TU Graz, and that it provides a comprehensive overview of RFID applications and security. The article also mentions that the school is held from July 12th to 14th, 2006, and that it is a great opportunity for students to gain practical experience in the field.

## APA-IT

The screenshot shows the APA-IT website's news section. The main headline is 'RFID-Sommerschule und Workshop in Graz'. The text describes the RFID Summer School as a future-oriented event that will focus on the identification of goods and animals using RFID technology. It mentions that the school is organized by Philips and TU Graz, and that it will provide a comprehensive overview of RFID applications and security. The article also notes that the school is held from July 12th to 14th, 2006, and that it is a great opportunity for students to gain practical experience in the field.