stiftung secure information and communication

Jahresbericht 2008

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 2008 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 Best Project Award 8
2.1.3 Vorlesung Kritische Informationsinfrastrukturen 9
2.1.4 E-Government 9
2.2 Eigenständige Forschung und Entwicklung 9
2.2.1 Forschung zu elektronischen Signaturen und eID 9
2.3 Organisatorisches und Sonstiges 9
2.3.1 Technische Infrastruktur 9
2.3.2 Entwicklungsaktivitäten JCE Toolkit 10

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 13. Juni 2009

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 2008 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2008 dar. Der Bericht behält die Struktur der bisherigen Berichte.

Im Berichtszeitraum konnte die Stiftung in allen Bereichen des Stiftungszwecks wertvolle Beiträge leisten:

- Die „*Stiftungsprofessur Informationssicherheit*“, die von der Stiftung SIC 2004 initiiert wurde und seit 2006 als permanente Professur besteht, wurde 2008 weiter getragen. Die Stelle von Prof. Vincent Rijmen wird bis September 2009 von der Stiftung zur Gänze finanziert, danach bis 2012 in einer Teilfinanzierung.

- Ein „*Best Project Award*“ wurde ausgeschrieben. Damit sollen vor allem Bakkalaureats- und Master-Studenten angeregt werden, in ihrem Studium qualitätsvolle Projekte aus Informationssicherheit zu beginnen.

- Aus dem Bereich Lehre wurde eine Lehrveranstaltung „*Kritische Informationsinfrastrukturen*“ an der TU Graz finanziert. Diese Lehrveranstaltung wurde im Wintersemester 2007/2008 zum zweiten Mal abgehalten.

- Im Bereich E-Government hat sich die Stiftung zusammen mit der TU Graz an Projekten des Landes Steiermark und des Bundes beteiligt.

- Aus dem Hilfsbetrieb JCE Toolkit konnten wiederum Gewinne erzielt werden, die dem gemeinnützigen Forschungsbereich zufließen.

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 2008 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 vom 21. April 2009 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 Erträgnissen 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 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 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 sechs 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.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2008 über die Stiftungsprofessur Kryptographie, die Lehrveranstaltung kritische Informationsinfrastrukturen, sowie einen neu ausgeschriebenen Best Project Award vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung. Aus der Stiftungsprofessur wurden wieder exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung wurde vorsichtig niedrig gehalten. Wissenschaftliche Weiterentwicklungen und notwendige Support- und Wartungsaufgaben wurden 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 Erträgnisse 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 ist seit 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).

1.5 Stiftungsorgane und Organisationsstruktur

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

o Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.

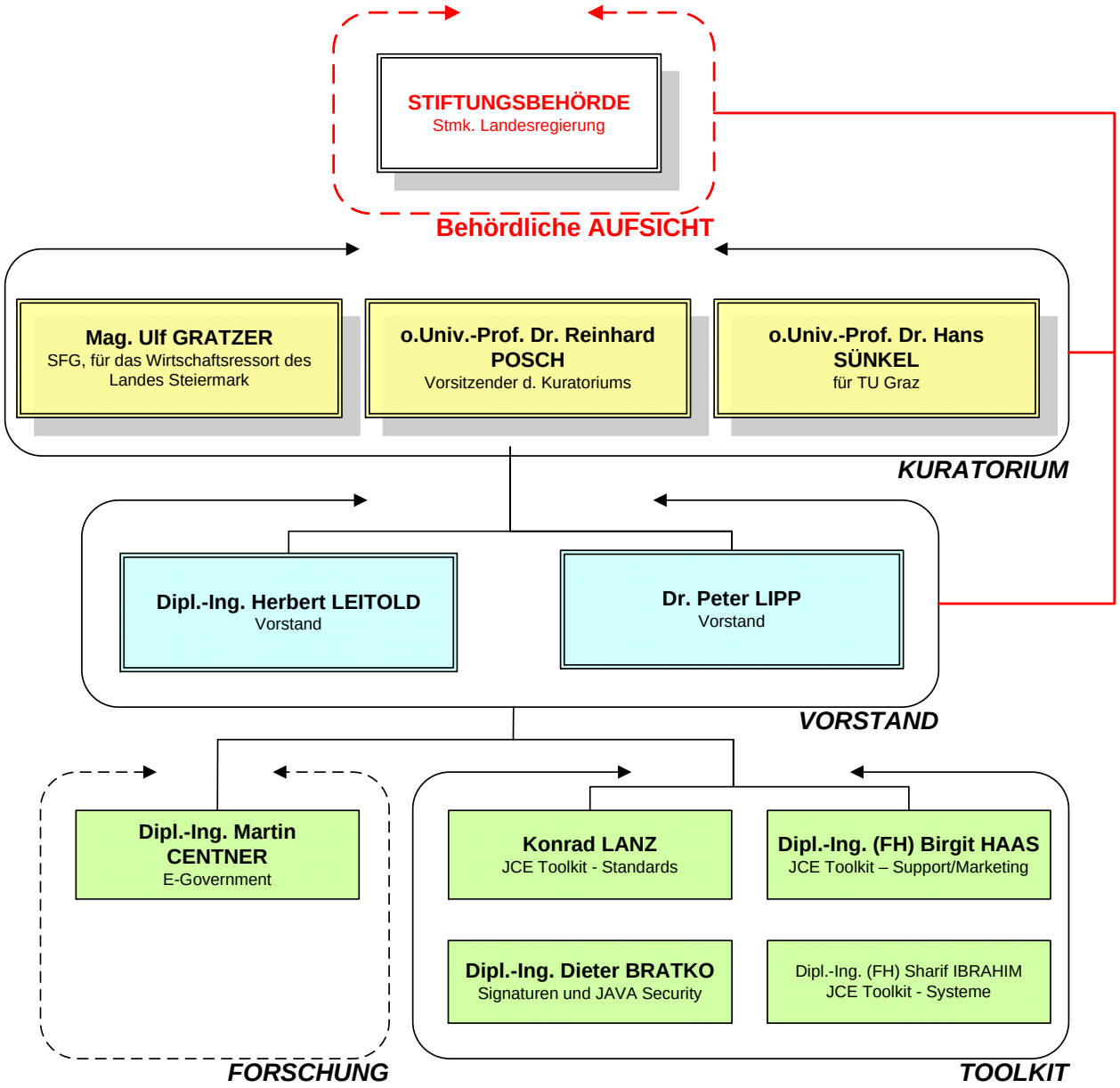
- Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2008 waren dies:
  - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
  - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
  - o.Univ.-Prof. Dr. Hans Sünkel (für die TU Graz)

- Staatliche Aufsicht ist die Stiftungsbehörde FA7C der Steiermärkischen Landesregierung

o Die Führungsebene bildet der Vorstand
  - Dipl.-Ing. Herbert Leitold
  - Dr. Peter Lipp

o 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 31.12.2008 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2008

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.

Seit 2006 ist die Professur an der TU Graz permanent eingerichtet. Die Stiftung hat eine Finanzierungszusage bis September 2009 bzw. eine Teil-Finanzierungszusage bis 2012 gegeben.

Seit Oktober 2007 ist die Stiftungsprofessur an der TU Graz nur mehr zu 30 % besetzt, die Initiative besteht jedoch weiter und 2008 konnte die Gruppe zahlreiche wissenschaftliche Schriften veröffentlichen oder war Co-Autor von wissenschaftlichen Publikationen:

1. Dipanwita Roy Chowdhury, Vincent Rijmen, Abhijit Das - "Progress in Cryptology - INDOCRYPT 2008" (Springer Berlin / Heidelberg - ISBN: 978-3-540-89753-8)

2. Marko Hölbl, Christian Rechberger, Tatjana Welzer - "Searching for messages conforming to arbitrary sets of conditions in SHA-256" - Proceedings of Western European Workshop on Research in Cryptology

3. Florian Mendel, Martin Schläffer - "Collisions for Round-Reduced LAKE" - Information Security and Privacy

4. Svetla Nikova, Vincent Rijmen, Martin Schläffer - "Using Normal Bases for Compact Hardware Implementations of the AES S-box" - Security and Cryptography for Networks

5. Christophe De Cannière, Christian Rechberger - "Preimages for Reduced SHA-0 and SHA-1" - Advances in Cryptology - CRYPTO 2008

6. Florian Mendel, Norbert Pramstaller, Christian Rechberger, Marcin Kontak, Janusz Szmidt - "Cryptanalysis of the GOST Hash Function" - Advances in Cryptology - CRYPTO 2008

7. Sebastiaan Indesteege, Florian Mendel, Bart Preneel, Christian Rechberger - "Collisions and other Non-Random Properties for Step-Reduced SHA-256" - Selected Areas in Cryptography (Note: to appear)

8. Emilia Käsper, Vincent Rijmen, Tor E. Bjørstad, Christian Rechberger, Matt Robshaw, Gautham Sekar - "Correlated Keystreams in MOUSTIQUE" - Progress in Cryptology – AFRICACRYPT 2008

9. Jean-Philippe Aumasson, Willi Meier, Florian Mendel - "Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5" - Selected Areas in Cryptography (Note: to appear)

10. Svetla Nikova, Vincent Rijmen, Martin Schläffer - "Secure Hardware Implementations of Non-Linear Functions in the Presence of Glitches" - Information Security and Cryptology - ICISC 2008

11. Florian Mendel, Norbert Pramstaller, Christian Rechberger - "A (Second) Preimage Attack on the GOST Hash Function" - Fast Software Encryption

12. ChangKyun Kim, Martin Schläffer, SangJae Moon - "Differential Side Channel Analysis Attacks on FPGA Implementations of ARIA" - ETRI journal information, telecommunications & electronics (Volume: 30 2)

13. Vincent Rijmen, Paulo S.L.M. Barreto, Decio Gazzoni Filho - "Rotation symmetry in algebraically generated cryptographic substitution tables" - Information processing letters devoted to the rapid publication of short contributions to information processing (Volume: 106 6)

14. Christian Rechberger, Vincent Rijmen - "New Results on NMAC/HMAC when Instantiated with Popular Hash Functions" - Journal of universal computer science (Volume: 14 3)

15. Mario Lamberger, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen - "Analysis of the Hash Function Design Strategy called SMASH" - IEEE transactions on information theory a journal devoted to the theoretical and experimental aspects of information transmission, processing, and utilization (Volume: 54)

Die Forschung zu Kollisionen von SHA-1 wurde 2008 fortgesetzt. SHA-1 ist eine der wesentlichsten Hash-Funktionen im Bereich der elektronischen Signatur. An einer von der Gruppe um Prof. Rijmen gestarteten, übers Internet verteilten Suche nach Kollisionen waren Ende 2008 bereits etwa 13.000 Benutzer und etwa 27.000 Rechner beteiligt.

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „Angewandte Kryptographie“ und „Angewandte Kryptographie 2“, „Einführung in die Informations-sicherheit“ „Cryptanalysis of symmetric cryptographic primitives (PV)“ und „IT-Sicherheit“ betreut. Das Angebot wird mit Seminaren, Projekten und Diplomarbeiten ergänzt.

Die von der Stiftung finanzierte Professur ist also als Nukleus erstklassischer Forschung im Bereich der Kryptographie anzusehen. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die mittlerweile internationales Ansehen genießt.

2.1.2 Best Project Award

Im Jahr 2008 wurde ein Best Project Award ausgeschrieben. Dieser soll Bakkalaureats- und Master-Studierende für die Beschäftigung mit Themen aus dem Stiftungszweck interessieren. Es werden Projekte mit Sachpreisen (z.B. einem Notebook) prämiert. Der Preis wurde Ende 2008 angekündigt und im Studienjahr 2009 gestartet. Die Vergabe erfolgt demnach erst 2009 nach dem Berichtszeitraum dieses Jahresberichts.

2.1.3 Vorlesung Kritische Informationsinfrastrukturen

Bereits im Wintersemester 2006/2007 wurde eine Vorlesung zu kritischen Informationsinfrastrukturen an der TU Graz gestartet und von der Stiftung finanziert. Mit Dr. Otto Hellwig konnte ein Vortragender gewonnen werden, der aus seiner beruflichen Tätigkeit im Bundeskanzleramt eine reichhaltige Erfahrung in diesem, angesichts der zunehmenden Abhängigkeit von Informationstechnologien immens in der Bedeutung steigenden Bereich, mitbringt.

Es wurde damit den Studierenden der TU Graz eine Bereicherung der Möglichkeiten in einem Feld angeboten, das erst an sehr wenigen Universitäten unterrichtet wird. Damit leistet die Stiftung einen Beitrag, Studierende konkurrenzfähig auszubilden.

Die Vorlesung Kritische Informationsinfrastrukturen wurde von der TU Graz auch im Wintersemsemester 2007/2008 angeboten bzw. wurde im Wintersemester 2008/2009 fortgesetzt. .

2.1.4 E-Government

Mitarbeiter des Bereichs Forschung der Stiftung unterstützen das E-Government Innovationszentrum (EGIZ). EGIZ ist eine Initiative des Bundeskanzleramts und der TU Graz zur wissenschaftlichen Weiterentwicklung des E-Government in Österreich. Experten der Stiftung werden zu Projekten beigezogen.

2.2 Eigenständige Forschung und Entwicklung

2.2.1 Forschung zu elektronischen Signaturen und eID

Forschung wurde im Bereich elektronischer Signaturen und elektronischer Identität betrieben. Dabei wurden folgende Aktivitäten durchgeführt:

- Analyse von Trust Service Status Listen
  Interoperabilität elektronischer Signaturen im grenzüberschreitenden Kontext bedarf automatisierter Entscheidung, ob Zertifikate von vertrauenswürdigen Zertifizierungsdiensteanbietern ausgestellt sind. In der Aktivität wurde analysiert, wie und welche bestehenden Standards dies unterstützen.
  ,
- Chipkarten-Integration in Browsern
  Es wurde untersucht, inwieweit aktuelle Browser über Technologien wie .net, javascript oder java applets die Integration von Chipkarten in Web-Anwendungen erlauben.

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.

2.3.1 Technische Infrastruktur

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 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 waren 2008 den Erwartungen entsprechend, Es wurden wiederum Entwicklungen teilweise von eigenem Personal der Stiftung, teilweise durch Forscher des IAIK übernommen. Dabei wurde das Toolkit vor allem wissenschaftlich weiter entwickelt, um über neue Funktionalitäten den Kundenerwartungen nach Unterstützung aktueller Entwicklungen der Informations-technologie zu genügen.