

# Jahresbericht 2011

## 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 2011 dargestellt.

## 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 Stiftungsprofessur Cloud Computing Security	8
2.1.3 JCE Toolkit unter EU-PL	8
2.1.4 Best Project Award	8
2.1.5 Vorlesung Kritische Informationsinfrastrukturen	8
2.1.6 E-Government	9
2.1.7 Eigene Forschungsleistungen	9
2.2 Organisatorisches und Sonstiges	9
2.2.1 Technische Infrastruktur	9
2.2.2 Entwicklungsaktivitäten JCE Toolkit	9

## 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 19/ Juni 2012



## 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 2011 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2011 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2011 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Die „*Stiftungsprofessur Informationssicherheit*“, die von der Stiftung SIC 2004 initiiert wurde und seit 2006 als permanente Professur besteht, wurde auch 2011 im Ausmaß von 50 % getragen.
- Eine weitere Stiftungsprofessur „*Cloud Computing Security*“ wurde vorbereitet und befindet sich mit dem Ziel Start 2013 in Ausschreibung.
- Das JCE Toolkit steht nun EU-PL Open Source Projekten kostenlos zur Verfügung. Dies kommt etwa im österreichischen E-Government zum Einsatz.
- In der Unterstützung von Studierenden wurden drei StudentInnen mit einem Best@IAIK Award ausgezeichnet. Weiters wurden drei Studenten unterstützt, um an der ETISS Summer School teilnehmen zu können.
- Im Bereich Lehre wurde weiterhin die Lehrveranstaltung „*Kritische Informationsinfrastrukturen*“ an der TU Graz finanziert.
- Der Hilfsbetrieb JCE Toolkit hat wiederum Gewinne erwirtschaftet, 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 2011 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 22. Mai 2012 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 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
- Cloud Computing
- 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**

Seit Bestehen der Stiftung wurde über Forschungsförderungen, Zuwendungen, Kooperationen und Gewinne des Hilfsbetriebs Toolkit ein Vermögensstand aufgebaut, der über das gewidmete Stammkapital hinausgeht. Trotz seit längerem anhaltend geringen Zinsniveaus konnten die Leistungen uneingeschränkt beibehalten werden. Durch die Rücklagen ist in absehbarer Zukunft auch mit keiner Änderung dieser Situation zu rechnen, sodass für Leistungen weiterhin nicht auf das Stammvermögen zurückgegriffen werden wird müssen.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2011 über die Stiftungsprofessur Kryptographie (seit Oktober 2008 in Teilfinanzierung), die Lehrveranstaltung kritische Informationsinfrastrukturen, sowie Best Project Awards und Förderungen von Summer Schools vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Aus der Stiftungsprofessur Kryptographie wurden wieder exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt.

Eine weitere Stiftungsprofessur „Cloud Computing Security“ ist in Vorbereitung, hat im Berichtszeitraum 2011 aber noch keine Kosten verursacht bzw. sind angesichts des geplanten Start 2013 auch noch keine Leistungen zu berichten.

Der Hilfsbetrieb „JCE Toolkit“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung ist leicht gesunken.

### **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 ist seit 2004 in der Satzung verankert.



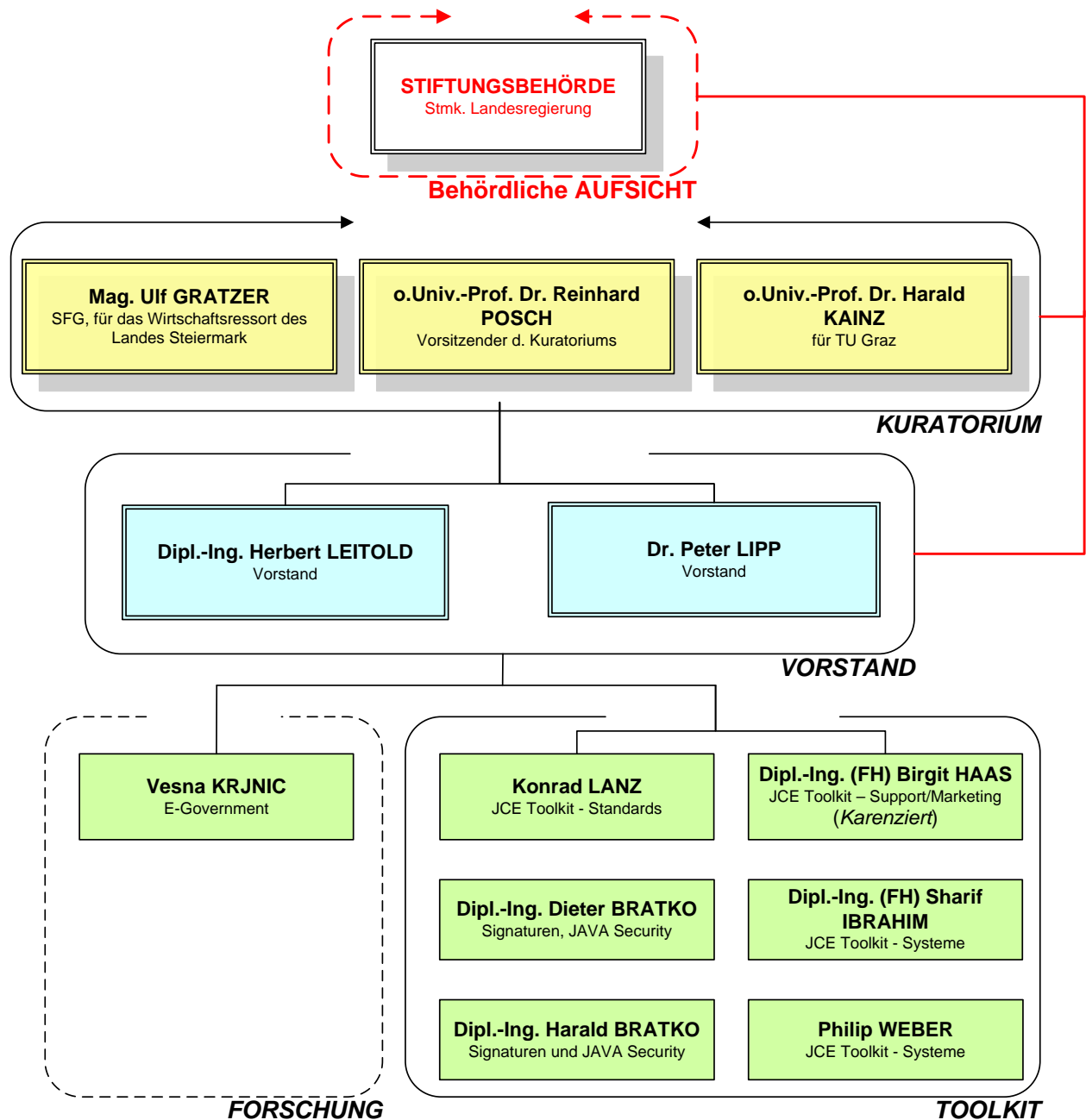
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

## 1.5 **Stiftungsorgane und Organisationsstruktur**

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2011 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, bis 1. Oktober 2011)
    - o.Univ.-Prof. Dr.techn. Dr.h.c. Harald Kainz (für die TU Graz, ab 1. Oktober)
  - 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 31.12.2011 dargestellt. Administration und technische Infrastruktur wird gegen Kostensatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2011



## 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“ 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 (seit 2009 zu 50 %), 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 2010 bzw. eine Teil-Finanzierungszusage bis 2013 gegeben.

Seit Oktober 2008 ist die Stiftungsprofessur an der TU Graz nur mehr zu 30 % besetzt, die Initiative besteht jedoch weiter und 2011 konnte die Gruppe zahlreiche wissenschaftliche Schriften veröffentlichen oder war Co-Autor von wissenschaftlichen Publikationen:

Es wurde eine Dissertation abgeschlossen:

1. Martin Schläffer - "Cryptanalysis of AES-Based Hash Functions"

Es wurden ein Artikel im Journal of Cryptology veröffentlicht:

1. Svetla Nikova, Vincent Rijmen, Martin Schläffer - "Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches" - Journal of cryptology (Volume: 24 2)

Weiters wurden sieben Artikel in Tagungsbänden wissenschaftlicher Konferenzen bereits veröffentlicht oder zur Veröffentlichung angenommen:

1. Florian Mendel, Tomislav Nad, Martin Schläffer - "Finding SHA-2 Characteristics: Searching Through a Minefield of Contradictions" - Advances in Cryptology - ASIACRYPT 2011
2. Kazumaro Aoki, Günther Roland, Yu Sasaki, Martin Schläffer - "Byte Slicing Grøstl - Optimized Intel AES-NI and 8-bit Implementations of the SHA-3 Finalist Grøstl" (to appear)
3. Florian Mendel, Tomislav Nad, Martin Schläffer - "Cryptanalysis of Round-Reduced HAS-160" - Information Security and Cryptology - ICISC 2011 (to appear)
4. Alex Biryukov, Mario Lamberger, Florian Mendel, Ivica Nikolic - "Second-Order Differential Collisions for Reduced SHA-256" – ASIACRYPT
5. Jérémy Jean, María Naya-Plasencia, Martin Schläffer - "Improved Analysis of ECHO-256" - SAC (to appear)



6. Tomislav Nad, Florian Mendel - "Boomerang Distinguisher for the SIMD-512 Compression Function" - Progress in Cryptology - INDOCRYPT 2011
7. Stefan Kölbl, Florian Mendel - "Practical Attacks on the Maelstrom-0 Compression Function" - Applied Cryptography and Network Security

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

Die von der Stiftung mit-finanzierte Professur ist also als Quelle 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 Stiftungsprofessur Cloud Computing Security**

Die Stiftungsprofessur Informationssicherheit war ein Erfolg. Da die Stiftung hinreichend Rücklagen ausbilden konnte, ist eine weitere Stiftungsprofessur „Cloud Computing Security“ an der TU Graz in Vorbereitung. Ziel ist der Start der Professur 2013.

Es wird das Modell einer Anschubfinanzierung verfolgt, in der kostenteilig die Stiftung anfangs einen wesentlichen Teil der Professur trägt und die TU Graz die Professur zusätzlich ausstattet. Über einen Zeitraum von sechs Jahren wird die Teilfinanzierung teils reduziert erhalten und soll danach von der TU Graz weiter getragen werden.

### **2.1.3 JCE Toolkit unter EU-PL**

Das JCE Toolkit der Stiftung kann seit 2011 auch von Open Source Projekten, die die EU-PL Lizenz verwenden, kostenlos eingesetzt werden. Eine bisher GPLv2 definierte Lizenz wurde auch EU-PL erweitert. Dies ist ein weiterer Schritt zur Förderung von Open Source Projekten und wurde etwa im österreichischen E-Government aufgegriffen, wo nun viele Module unter EU-PL gestellt wurden.

### **2.1.4 Best Project Award**

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2011 wurden Preise an drei Studierende der TU Graz vergeben:

1. Beste Ferialarbeit: Alexander Marsalek für „Android Market Application Watcher“
2. Beste Bakkalaureatsarbeit: Maria Eichlseder für ihre Arbeit „Memoryless Near-Collisions via Coding Theory“
3. Beste Masterarbeit: Heinz Riener für seine Arbeit „Formal Methods for the Analysis of Program Mutations“

Weiters wurden drei Studierende bei der Teilnahme der Sommerschule ETISS „6<sup>th</sup> European Trusted Infrastructure Summer School“ in Darmstadt unterstützt.

### **2.1.5 Vorlesung Kritische Informationsinfrastrukturen**

Die Vorlesung über kritische Informationsinfrastrukturen an der TU Graz wurde von der Stiftung zum fünften Mal finanziert. Die Vorlesung wurde wieder von Dr. Otto Hellwig gehalten.





### **2.1.6 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.

### **2.1.7 Eigene Forschungsleistungen**

Mitarbeiter der Stiftung haben eigenständige Forschung im Bereich elektronischer Signaturen und Notfallsysteme zu Public Key Infrastrukturen durchgeführt. Dazu erfolgt eine zeitweise Freistellung von Aufgaben im Bereich Toolkit.

## **2.2 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.

### **2.2.1 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.

### **2.2.2 Entwicklungsaktivitäten JCE Toolkit**

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2011 im Rahmen der Erwartungen. Diese wurden aus Aufträgen im ETSI Standardisierungsmandat zu elektronischen Signaturen übertroffen. Die Stiftung hat dabei teilweise Leistungen von Experten der TU Graz bezogen.