stiftung secure information and communication

Jahresbericht 2013

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 2013 dargestellt.

Inhaltsverzeichnis

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 15/ Juni 2014

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 „*…eigenständige Durchführung von Forschungsaufgaben und -projekten, Förderung anderer Einrichtungen, Personen und Institutionen, die zur Erreichung des Stiftungszweckes beitragen, Vergabe von Forschungsaufträgen, Vergabe von Beiträgen für wissenschaftliche Arbeiten, Durchführung von Veranstaltungen zur Bekanntmachung der Forschungsergebnisse, Publikation und Dokumentation der im Rahmen des Stiftungszwecks durchgeführten Forschungstätigkeiten*“ erfolgen.

Dieser Jahresbericht 2013 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2013 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2013 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Die „*Stiftungsprofessur Informationssicherheit*“, die von der Stiftung SIC 2004 initiiert wurde, wurde über eine Gastprofessur zu 50 % finanziert.
- Eine weitere Stiftungsprofessur „*Cloud Computing Security*“ wurde eingerichtet. Sie wurde mit Prof. Mangard besetzt und wird zu 67% finanziert,
- In der Unterstützung von Studierenden wurden drei StudentInnen mit einem Best@IAIK Award ausgezeichnet bzw. eine Konferenzreise unterstützt.
- Die Stiftung hat die wirtschaftliche Abwicklung und Ausfallshaftung für die ETISS (European Trusted Infrastructures and Systems School) und die INTRUST-Konferenz, die in Graz abgehalten wurden, übernommen.
- Die Stiftung hat sich im EU Projekt STORK 2.0 beteiligt. Es ist dies ein Large Scale Pilot zur Interoperabilität elektronischer Identität.
- 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 2013 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 27. Juni 2014 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 (aktuelle Version vom 7.11.2013) wie folgt definiert:

> *Zweck der Stiftung, die nicht auf Gewinn gerichtet ist, 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 Informations-sicherheit.*
>
> *Das Ziel der Stiftung ist die Erweiterung des menschlichen Wissens in den oben genannten Bereichen im Interesse der österreichischen Allgemeinheit.*

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 Informations-verarbeitung, 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 wissen-schaftlichen 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. Es ist in absehbarer Zukunft nicht damit zu rechnen, dass für Leistungen auf das Stammvermögen zurückgegriffen werden wird müssen.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2013 über die Stiftungsprofessur Kryptographie (von Oktober 2008 bis September 2013 in Teilfinanzierung), die Stiftungsprofessur Cloud Computing (2013 eingerichtet), die Lehrveranstaltung kritische Informationsinfrastrukturen, sowie Best Project Awards 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“ wurde eingerichtet. Diese wurde erst im November 2013 gestartet. .

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

Es bestehen also ausreichend Reserven, um die Leistungen der Stiftung weiterhin auf hohem Niveau halten zu können.

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),

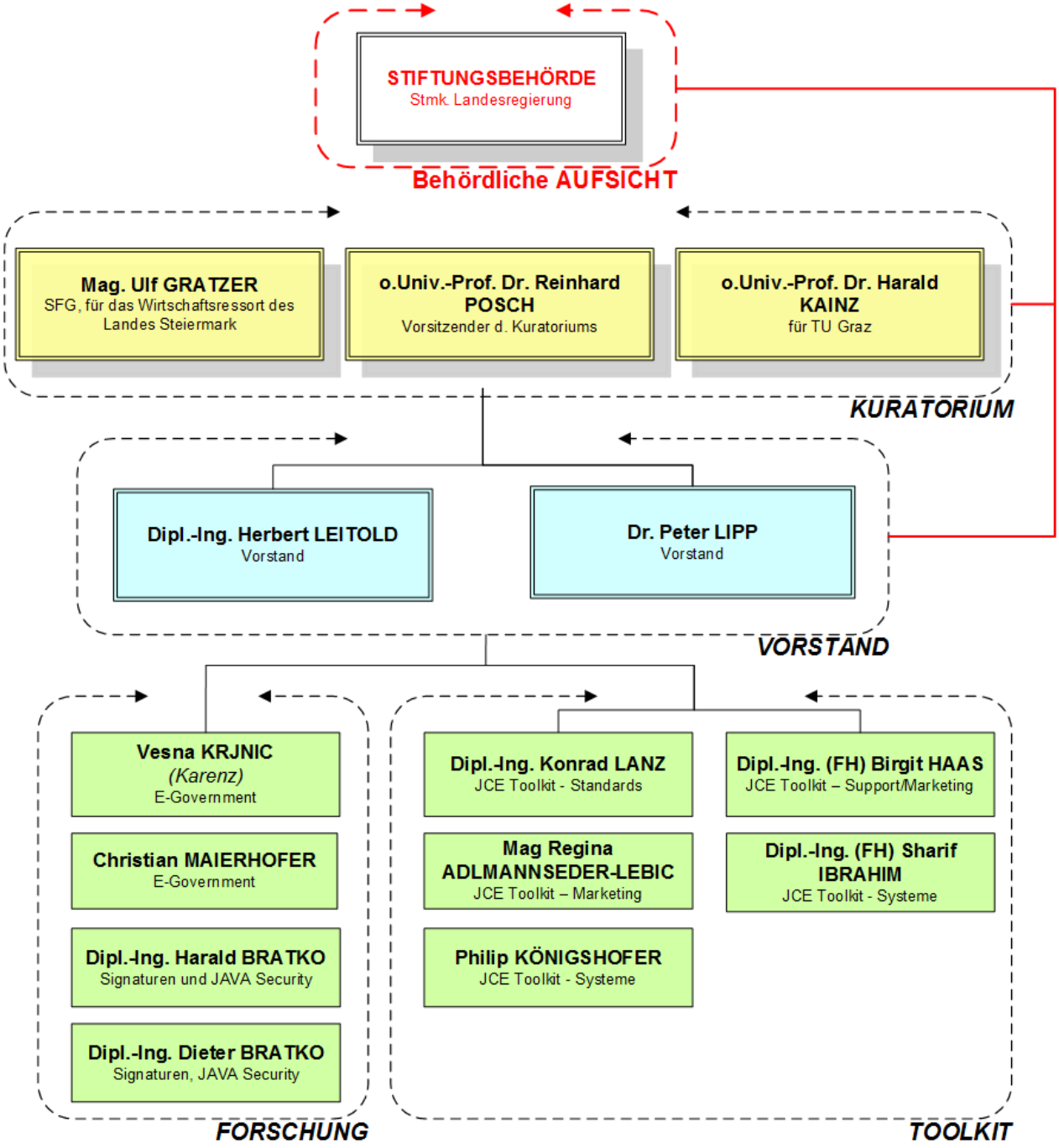
„Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

1.5 Stiftungsorgane und Organisationsstruktur

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2013 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
    - o.Univ.-Prof. Dr.techn. Dr.h.c. Harald Kainz (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 31.12.2013 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2013

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

Mit 1.10.2004 wurde die Stiftungsprofessur Informationssicherheit eingerichtet. Diese wurde bis 2010 voll, bis September 2013 zu 50% finanziert, die TU Graz stattet die Stiftungsprofessur mit Räumlichkeiten, AssistentInnen und Sekretariat aus.

Seit 2006 ist die Professur an der TU Graz permanent eingerichtet. Die Stiftung hat eine Finanzierungszusage bis September 2012 bzw. eine Teil-Finanzierungszusage bis 2013 gegeben.

Nach Wechsel Prof. Rijmen 2012 an die KU Leuven wurde als Ersatz eine Gastprofessur eingerichtet, die mit Dr. Florian Mendel besetzt wurde. Die Stiftungsprofessur wurde von der TU Graz 2013 neu ausgeschrieben.

Auch 2013 konnte die Gruppe zahlreiche wissenschaftliche Schriften veröffentlichen oder war Co-Autor von wissenschaftlichen Publikationen:

Es wurde ein Journal-Artikel zur Veröffentlichung angenommen:

1. Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, Martin Schläffer - "The Rebound Attack and Subspace Distinguishers: Application to Whirlpool" - Journal of cryptology (to appear)

Weiters wurden sieben Artikel in Tagungsbänden wissenschaftlicher Konferenzen veröffentlicht:

1. Florian Mendel, Tomislav Nad, Martin Schläffer - "Finding Collisions for Round-Reduced SM3" - Topics in Cryptology - CT-RSA 2013

2. Florian Mendel, Thomas Peyrin, Martin Schläffer, Lei Wang , Shuang Wu - "Improved Cryptanalysis of Reduced RIPEMD-160" - Advances in Cryptology - ASIACRYPT 2013

3. Florian Mendel, Tomislav Nad, Martin Schläffer - "Improving Local Collisions: New Attacks on Reduced SHA-256" - Advances in Cryptology – EUROCRYPT 2013

4. Begul Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel, Qingju Wang - "FIDES: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware" - Cryptographic Hardware and Embedded Systems - CHES 2013 Icon BibTex Icon Download Icon WebUrl

5. Maria Eichlseder, Florian Mendel, Tomislav Nad, Vincent Rijmen, Martin Schläffer - "Linear Propagation in Efficient Guess-and-Determine Attacks" - International Workshop on Coding and Cryptography

6. Stefan Kölbl, Florian Mendel, Tomislav Nad, Martin Schläffer - "Differential Cryptanalysis of Keccak Variants" - Cryptography and Coding

7. Florian Mendel, Vincent Rijmen, Deniz Toz, Kerem Varici - "Collisions for the WIDEA-8 Compression Function" - Topics in Cryptology - CT-RSA 2013

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.

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

Eine weitere Stiftungsprofessur *Cloud Computing* wurde mit November 2013 mit Prof. Stefan Mangard besetzt. Die Stiftung wird diese Professur auf drei Jahre zu 67% finanzieren sowie auf weitere drei Jahre zu 33%. Zusätzlich finanziert die Stiftung 67% einer Stelle eines/einer UniversitätsassistentIn auf sechs Jahre.

Aus der kurzen Besetzungszeit im Berichtszeitraum von zwei Monaten (November-Dezember) sind noch keine Veröffentlichungen entstanden.

2.1.3 Best Project Award

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2013 wurden Preise an drei Studierende der TU Graz vergeben:

1. Beste Ferialarbeit: Timotheus Hell für seine Arbeit „Setting up the Synthesis Competition“

2. Beste Bakkalaureats-Arbeit: Felix Hörander für seine Arbeit „Secure Cloud Storage Using the SkyTrust System“

3. Beste Masterarbeit: Wolfgang Wieser für seine Arbeit „Repairing Boomerang Characteristics“

Zusätzlich wurde die Teilnahme an der Apple World Wide Developer Konferenz durch Herrn Christof Stromberger über einen Reisezuschuss unterstützt.

2.1.4 ETISS/INTRUST 2013 in Graz

Im Dezember 2013 fanden in Graz die ETISS (European Trusted Infrastructures and Systems School) sowie die INTRUST-Konferenz statt. Da die Finanzierung der ETISS, an der Studierende kostenlos teilnehmen können, nicht wie in den Jahren davor durch Spenden von namhaften Firmen gesichert war, hat die Stiftung Ausfallshaftung für die Veranstaltung sowie die wirtschaftliche und organisatorische Abwicklung übernommen.

Dank intensiver Bemühungen des Organisationsteams konnten mit Spenden von HP und Microsoft doch genügend Mittel geworben werden, die es uns erlaubten, die Abhaltung für alle Studierenden kostenlos zu halten sowie die Hotel- und Verpflegungskosten zu tragen, sodass die TeilnehmerInnen lediglich die Anreisekosten übernehmen mussten.

Als Teil der ETISS wurde die INTRUST-Konferenz abgehalten, die ein wenig an mangelnden Einreichzahlen litt. Die Qualität der angenommenen Beiträge war jedoch gut.

Wirtschaftlich erreichten die Ausgaben für die Veranstaltung nicht die Spendensumme der Firmen, sodass die Ausfallshaftung nicht schlagend wurde. Der entstandene Überschuss ist für Finanzierung von Teilnahmen Studierender an künftigen ETISS- oder ähnlichen Veranstaltungen vorgesehen.

2.1.5 STORK 2.0

Die Stiftung nimmt am EU Projekt STORK 2.0 teil. Es ist dies ein von der Europäischen Kommission geförderter Large Scale Pilot zur Interoperabilität elektronsicher Identität. Die Teilnahme der Stiftung erfolgt über eine Arbeitsgemeinschaft „ARGE STORK.AT“ zusammen mit dem Bundeskanzleramt, dem Bundesministerium für Gesundheit, der TU Graz, der ELGA GmbH und A-SIT.

2.1.6 Vorlesung Kritische Informationsinfrastrukturen

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

2.1.7 E-Government

MitarbeiterInnen 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.

2.1.8 Eigene Forschungsleistungen

Mitarbeiter der Stiftung haben eigenständige Forschung im Bereich mobiler elektronischer Identität und Signaturen durchgeführt. Es wurde eine Lösung für server-basierte Signaturen mit Autorisierung über das Mobiltelefon entwickelt. 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 2013 etwas unter den Erwartungen. Diese wurden über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen ergänzt. Die Stiftung hat dabei teilweise Leistungen von Experten der TU Graz bezogen.