Jahresbericht 2003

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

Die *Stiftung Secure Information and Communication Technologies SIC* – in Folge als „die Stiftung" bezeichnet – wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität 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 ihrem Gründungsjahr berichtet.

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)

Executive Summary

Die Stiftung Secure Information and Communication Technologies SIC wurde im Februar 2003 gegründet und mit einem Stammvermögen von € 2.320.000 ausgestattet. Gemäß Satzung ist der Zweck der Stiftung „*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*“.

In ihrem Gründungsjahr hat die Stiftung in allen im Stiftungszweck genannten Aspekten Impulse gesetzt und Leistungen erbracht. Dies wird in diesem Jahresbericht dargestellt.

In der Förderung von Forschung und Lehre wurde vor allem die Errichtung einer „*Stiftungsprofessur Informationssicherheit*“ an der TU Graz vorbereitet. Damit soll über eine Professur Forschung und Lehre in den Bereichen des Stiftungszwecks nachhaltig gestärkt werden. Diese Stiftungsprofessur, dessen Vorfeldtätigkeiten 2003 begannen, soll 2004 eingerichtet werden.

Weiters war es im Bereich Forschung und Lehre auch möglich, mit Dr. Vincent Rijmen einen international höchst renommierten Forscher in einer Teilzeitposition nach Graz zu verpflichten, wodurch in der Steiermark sowohl in der universitären Lehre als auch in der Forschung neue Bereiche erschlossen werden konnten.

Um Studentinnen und Studenten anzuregen, sich in früh mit den von der Stiftung zu fördernden Bereichen wissenschaftlich zu beschäftigen und damit einen Impuls in ihrer Ausbildung zu setzen, wurde ein „*Best Paper Award*“ ausgeschrieben, deren Gewinner zu einer internationalen Fachkonferenz in die USA eingeladen wurde. Diese Initiative hat auch entsprechendes Medieninteresse ausgelöst.

In der eigenständig durchgeführten Forschung wurden unter den Kurzbezeichnungen POSITIF und TEJP zwei Forschungsprojekte zur Informationssicherheit definiert. Ersteres wurde zum 6. Rahmenprogramm der EU eingereicht und ausgewählt. Damit kann der Bereich Netzwerksicherheit auf eine Dauer von drei Jahren von der EU gefördert mit einem Budget von etwa € 300.000 bearbeitet werden.

Weiters wurde die Stiftung vom European Telecommunciation Standards Institute ETSI mit der Durchführung von Interoperabilitäts-Untersuchungen zu XML Signaturstandards beauftragt. Damit wurde eine Wissensbasis geschaffen, die für weitere Forschung und Entwicklungen genutzt werden kann.

Die finanzielle Lage der Stiftung ist als ausgezeichnet zu bezeichnen. Durch Zuwendungen konnte das Stiftungsvermögen am Ende des Berichtsjahrs per 31. Dezember 2003 auf € 2.770.000 gesteigert werden, mit Zuwendungen wie etwa die Rechte an einem eingeführten, kommerziell verwertbaren Softwareprodukt zur Informationssicherheit „*JCE Toolkit*“ weist die Stiftung für das Geschäftsjahr 2003 einen Bilanzgewinn von über € 49.000 aus. Mit der Einrichtung des Hilfsbetriebs „*JCE Toolkit*“ sind Leistungen der Stiftung, die über die rein aus den Erträgnissen der Veranlagung des pekuniären Stammvermögens hinausgehen, als nachhaltig gesichert anzusehen.

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 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 Gründungsjahr 2003 dargestellt.

Entsprechend Beschluss des Kuratoriums der Stiftung vom 23. März 2004 ist dieser Bericht im Internet zu veröffentlichen.

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. im Internet unter http://sic.iaik.tugraz.at/Satzung/ veröffentlicht.

1.2 Forschungsschwerpunkte

Die allgemeine Formulierung des Stiftungszwecks soll dem in der Informationsverarbeitung und 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 durch den Vorstand der Stiftung aktuelle Schwerpunkte definiert und diese vom Kuratorium der Stiftung bestätigt.

Als Forschungsschwerpunkte wurden 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
- 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 Allgemeines zur Lage der Stiftung

Im Gründungsjahr der Stiftung war parallel zur Leistungserbringung nach dem Stiftungszweck die administrative, organisatorische und technische Infrastruktur aufzubauen. Durch die Übertragung des so genannten „*JCE Toolkit*" durch das IAIK der TU Graz an die Stiftung (siehe Abschnitt „2.3.2 Entwicklungsaktivitäten JCE Toolkit") verfügt die Stiftung neben den Erträgnissen aus dem Stammvermögen über einen Hilfsbetrieb, dessen Gewinne zur Gänze dem gemeinnützigen Stiftungszweck zufließen und damit die Stiftung stärken. Dazu waren im Gründungsjahr die rechtlichen Grundlagen, vor allem der steuerrechtliche Status von gemeinnützigen und gewinnorientierten Aktivitäten, sowie die finanztechnische Abgrenzung dieser Bereiche zu klären.

Trotz dieser allgemeinen Aktivitäten kann die Stiftung bereits im ersten Jahr ihres Bestehens auf einige bemerkenswerte Leistungen verweisen, die im Verlauf dieses Berichts im Detail ausgeführt werden. In Kürze dargestellt waren die wesentlichen Aktivitäten des Jahres 2004:

- Die Ausschreibung eines Studentenwettbewerbs „*Best student paper award*", über den Studierende bereits in ihrer Ausbildung angeregt werden, sich mit den Fachgebieten des Stiftungszwecks auseinanderzusetzen. Der Gewinner wurde zur Teilnahme an einer renommierten wissenschaftlichen Fachtagung eingeladen.

- Die Vorbereitung zur Einrichtung einer „*Stiftungsprofessur Informationssicherheit*" an der TU Graz, über die die Forschung und Lehre in den Fachgebieten des Stiftungszwecks in Graz nachhaltig gestärkt werden soll.

- Zur „*Stärkung von Forschung und Lehre in der Informationssicherheit*" an der TU Graz konnte mit Dr. Vincent Rijmen eine international anerkannte Kapazität in eine Teilzeitverhältnis gewonnen werden. Dr. Rijmen hat die Forschung und Lehre in Graz in Bereichen des Stiftungszecks belebt.

- Die Stiftung hat an der ersten Ausschreibung zum 6. Rahmenprogramm der EU in einem internationalen Konsortium im „*Forschungsprojekt POSITIF*" teilgenommen. Dieses innovative Projekt wurde von der EU Kommission akzeptiert. Damit wird eigenständige Forschung in den Fachgebieten des Stiftungszwecks betrieben und durch EU Forschungsgelder zusätzlich abgesichert.

Es hat sich somit bereits im Gründungsjahr ein deutliches Profil der Stiftung hinsichtlich Förderung von Forschung und Lehre herausgebildet (Stiftungsprofessur und Studenten-wettbewerb). Es wurden auch erfolgreiche Impulse zur eigenständigen Durchführung von wissenschaftlicher Forschung gesetzt (Forschungsprojekt POSITIF).

Darüber hinausgehend hat sich der Vermögenstand durch eine Zuwendung des IAIK der TU Graz deutlich gesteigert. Zusammen mit den übertragenen Rechten am JCE Toolkit kann die Lage der Stiftung als ausgezeichnet bezeichnet werden. Konkret weist der Rechnungsabschluss aus:

Stammvermögen	€	2.320.000,00
Sonstiges Vermögen (Rücklage)	€	450.000,00
Bilanzgewinn	€	49.147,07
Eigenkapital	**€**	**2.819.147,07**

Trotz der aktuell zu wenig Euphorie einladenden Zins- und Renditenlage sind dadurch gemeinnützige Leistungen der Stiftung, die über die rein aus dem pekuniären Stamm-vermögen erzielbaren Erträgnisse hinausgehen, auch für die Folgejahre gesichert.

1.4 Organisationsstruktur

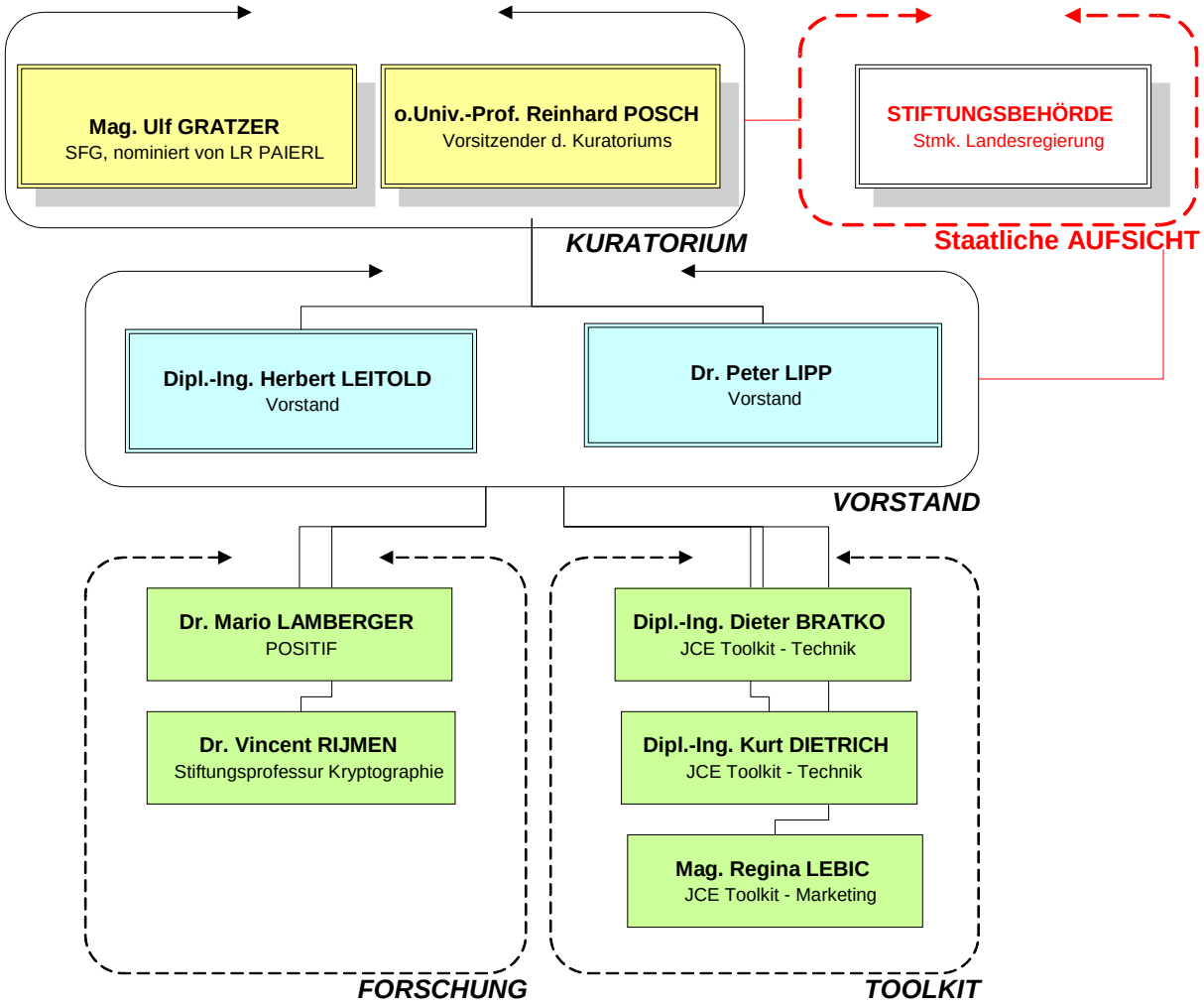
Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Vorsitzender des Kuratoriums ist o.Univ.-Prof. Dr. Reinhard Posch. Als zweites Mitglied des Kuratoriums wurde von Landesrat Dipl.-Ing. Herbert Paierl als dessen Stellvertreter [*Anm.*: *Name gelöscht*] nominiert. Seit 1.12.2003 nimmt diese Funktion Mag. Ulf Gratzer wahr
  - Staatliche Aufsicht ist die Stiftungsbehörde FA7C der Steiermärkischen Landesregierung

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

- Die operative Ebene wird durch zwei Säulen gebildet:
  - Der Bereich *Forschung* umfasst die mit eigenständiger Durchführung von Forschung und Entwicklung befassten Mitarbeiter der Stiftung.
  - Der Bereich *Toolkit* ist als gewinnorientierter Betrieb vom gemeinnützigen Bereich *Forschung* abgegrenzt, unterstützt diesen jedoch über Gewinne und in der Forschung verwendete Werkzeuge

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Mitarbeiterinnen- und Mitarbeiterstand der Stiftung per 31.12.2003 dargestellt, der Bereich Administration ist wie die technische Infrastruktur vom IAIK der TU Graz gestellt – die Kosten werden von der Stiftung ersetzt.



Die Aktivitäten der Stiftung im Berichtsjahr werden im folgenden Abschnitt detailliert.

2. Leistungen im Sinne des Stiftungszwecks

Die Leistungen der Stiftungen werden nach dem in der Satzung der Stiftung definierten *Stiftungszweck* in „*Förderung von Forschung und Lehre*“ und „*Eigenständige Forschung und Entwicklung*“ strukturiert berichtet. Zusätzlich werden in „*Organisatorisches und Sonstiges*“ jene Aktivitäten zusammengefasst, die sich aus dem im Gründungsjahr erforderlichen Aufbau der Infrastruktur bzw. den gewinnorientierten Aktivitäten im Betrieb JCE Toolkit ergeben.

2.1 Förderung von Forschung und Lehre

2.1.1 Best student paper award

Ein satzungsgemäßes Ziel der Stiftung ist die Förderung von Lehre und Wissenstransfer in der Informationssicherheit. Um Studentinnen und Studenten anzuregen, sich mit diesem Thema bereits während ihrer Ausbildung intensiv zu befassen, wurde ein Best Student Paper Award ausgeschrieben. Als attraktiver Preis wurde der Gewinnerin oder dem Gewinner die Wahl der Teilnahme (Finanzierung von Flug, Hotel und Konferenzgebühr) an einer der zwei folgenden renommierten Fachkonferenzen in den USA in Aussicht gestellt:

- CRYPTO’2003, Santa Barbara, CA, August 2003
- ACSAC’2003; Las Vegas, NV, Dezember 2003

Um ein breites studentische Feld zu erreichen, war der Wettbewerb nicht nur auf Studentinnen und Studenten beschränkt, die im Studium unmittelbar mit Informationstechnologien befasst sind, sondern wurde auf alle Studierende der TU Graz ausgeschrieben. Der Wettbewerb wurde Ende April 2003 gestartet. Zum Stichtag 27. Juni 2003 waren sechs Einreichungen eingelangt. Diese wurden von den Mitarbeiterinnen und Mitarbeitern des IAIK der TU Graz, des Zentrum für sichere Informationstechnologie – Austria A-SIT und den Vorständen der Stiftung begutachtet.

Aus diesem Prozess ging der Beitrag „*A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags*“ von Herrn Martin Feldhofer als Gewinner hervor. Herr Feldhofer wurde zur ACSAC’2003 in Las Vegas eingeladen. Der Beitrag ist am Internetauftritt der Stiftung http://www.sic.st veröffentlicht.

Der Best Student Paper Award erzielte auch entsprechendes Echo in den österreichischen Medien. Die Presseberichte werden im „Medienresonanz“ gegeben.

In der Begutachtung waren die befassten Personen einig, dass die Arbeit von so hoher Qualität ist, dass Herrn Feldhofer nahe gelegt wurde, sich weiter mit dem Thema zu beschäftigen und einen daraus resultierenden Beitrag auch bei einer wissenschaftlichen Fachkonferenz einzureichen. Dies war auch erfolgreich – der Beitrag wurde von der Fachjury zur Veröffentlichung bei der IEEE MELECON’2004 in Dubrovnik akzeptiert und wird dort im Mai 2004 präsentiert.

2.1.2 Stiftungsprofessur Informationssicherheit

Zur Förderung der Lehre in der Informationssicherheit wurde beschlossen, eine Stiftungsprofessur aus Informationssicherheit an der TU Graz einzurichten. Mit der Reorganisation der Universitäten durch das Universitätsgesetz 2002 wurde als vorteilhaft angesehen, diesen Prozess formell erst nach dem Übergang in die Vollrechtsfähigkeit zu starten, die Stiftungsprofessur also mit einer Ausschreibung im Jahr 2004 zu initiieren, die Vorfeldtätigkeiten dazu wurden bereits 2003 gestartet.

2.1.3 Stärkung von Forschung und Lehre in der Informationssicherheit

Mit Beginn des Wintersemesters 2003/2004 konnte mit Dr. Vincent Rijmen einer der europaweit potentesten Forscher in der Kryptographie in einem Teilzeitverhältnis an die Stiftung gebunden werden. Dr. Rijmen hat etwa die Lehrveranstaltung Angewandte Kryptographie 2003 gelesen.

In seinen Forschungsaktivitäten hat Dr. Rijmen mit der Kryptoanalyse von Hash-Funktionen begonnen, wie sie etwa im Bereich der elektronischen Signaturen notwendig sind. Eine

qualifizierte Aussage über deren Sicherheitsniveaus ist eine Grundlage zur Bewertung der Risken elektronischer Geschäftsprozesse. Erste Interimsresultate wurden noch nicht veröffentlicht. Dies erfolgt, sobald entsprechend fundierte Aussagen möglich sind.

Neben einer Vielzahl wissenschaftlicher Veröffentlichungen ist Dr. Vincent Rijmen vor allem deshalb bekannt, weil sich der von ihm zusammen mit Dr. Joan Daemen entworfene Algorithmus Rijndael im Jahr 2000 im von National Institute for Standards and Technology (NIST) ausgeschriebenen Wettbewerb um den Advanced Encryption Standard (AES) gegen die internationale Konkurrenz durchsetzen konnte.

Somit konnte eine international anerkannte Kapazität nach Graz geholt werden, die die Forschungs- und Lehrtätigkeit in Fachbereichen des Stiftungszwecks nachhaltig belebt. Es ist zu erwarten, dass Dr. Rijmen sich auch um die Stiftungsprofessur bewerben wird.

2.2 Eigenständige Forschung und Entwicklung

2.2.1 Forschungsprojekt POSITIF

Im Zuge der ersten Ausschreibung zu Forschungsprojekten im 6. EU Rahmenprogramm hat sich die Stiftung im Projektvorschlag „*Policy-based Security Tool and Framework (POSITIF)*“ beteiligt. Dieses Projekt wurde von der EU Kommission mit einem Projektstartzeitpunkt Anfang Februar 2004 akzeptiert. Das Projekt wird Forschung im Bereich Policy-orientierter Frameworks zu Netzwerksicherheit betreiben und Werkzeuge der Informationssicherheit entwickeln.

Über einen Projektzeitraum von drei Jahren steht der Stiftung ein voraussichtliches Budget in Höhe von insgesamt etwa € 300.000 zur Verfügung. Im so genannten Zusatzkostenmodell werden die Kosten der seitens der Stiftung zusätzlich eingebrachten Forschungskapazität durch die EU Förderung ersetzt. So konnte Dr. Mario Lamberger für diesen Forschungsbereich eingestellt werden. Es soll über die zusätzlich seitens der Stiftung eingebrachten Ressourcen ein Forschungsbereich in der Netzwerksicherheit etabliert werden.

2.2.2 Forschungsprojekt TEJP

Weiters wurde ein Projektantrag „*Trusted Embedded Java Platform (TEJP)*“ zur dritten Ausschreibung des österreichischen Forschungs-Förderprogramms FIT-IT Embedded Systems erarbeitet. Ziel dieses Projektes war, vertrauenswürdige Komponenten für mobile Endgeräte zu entwickeln, um damit in diesem dynamischen Segment Werkzeuge zu schaffen, effizient sichere Systeme zu entwickeln.

Dieses Projekt wurde unter FIT-IT nicht zur Förderung ausgewählt. Das vorläufige Review-Ergebnis zeigt, dass die Evaluatoren keine konkreten wissenschaftlichen Schwachpunkte identifizieren konnten, sondern den wirtschaftlichen Partner (Fa. XiCrypt) und dessen Kompetenz und Finanzkraft nicht kannten. Inwieweit die konzeptionellen Vorarbeiten als Basis eines durch Stiftungsmittel unterstützten Forschungsgebiets weiter verfolgt werden, wird derzeit untersucht.

2.2.3 XAdES Interoperability Tests

Im Rahmen der Mitarbeit in der Gruppe *ESI* (Electronic Signatures and Infrastructures) der ETSI entstand eine Initiative, die Interoperabilität der von Mitgliedern dieser Gruppe sowie der Industrie entwickelten Implementierungen des XAdES-Standards zur Langzeitsicherung elektronischer Signaturen zu untersuchen. Die Plugtests™ -Gruppe der ETSI unterstützte diesen Interoperabilitätstest organisatorisch und stellte ein Budget für die Umsetzung zur Verfügung. Die Leitung des Tests wurde von der Technischen Universität Barcelona (UPC) zusammen mit der Stiftung übernommen. Anfang November fand dann in Sophia Antipolis das mehrtägige Interop-Event statt.

2.3 Organisatorisches und Sonstiges

In diesem Abschnitt werden Aktivitäten berichtet, die zwar nicht in ursächlichem Zusammenhang mit dem gemeinnützigen Stiftungszweck stehen, jedoch als administrative und organisatorische Infrastruktur vor allem im Gründungsjahr erforderlich waren, um die Stiftungsaktivitäten effizient durchzuführen.

2.3.1 Technische Infrastruktur

Die technische Infrastruktur der Stiftung wird in den Anfangsphasen vor allem vom IAIK der TU Graz getragen. Es wurden sukzessive die für die eigenständige Durchführung der Forschung notwendigen Komponenten, vor allem PCs, aus Mitteln der Stiftung angeschafft. Durch die langjährig qualitativ hochwertig aufgebauten Ressourcen des IAIK vor allem im Netzwerk- und Serverbereich wird mittelfristig eine Mitbenutzung unter Kostenersatz ökonomisch sinnvoller sein, als hier den Aufbau eigener Ressourcen zu forcieren.

In die Infrastruktur des IAIK einbettet wurden ein Intranet bzw. unter der Domäne sic.st der öffentliche Webauftritt http://www.sic.st (bzw. http://sic.iaik.tugraz.at) gestartet.

2.3.2 Entwicklungsaktivitäten JCE Toolkit

Das JCE Toolkit wurde durch das IAIK der TU Graz per 15. Dezember 2003 an die Stiftung übertragen. Damit wurde der Stiftung ein eingeführter Betrieb zuerkannt, über dessen Gewinne Erträgnisse der Stiftung zu erwarten sind, die gänzlich dem gemeinnützigen Stiftungszweck zufließen.

Der nachhaltige Verkaufserfolg bedarf jedoch laufender Wartungs- und Entwicklungsarbeiten, zum Erhalt des Standes der Technik auch Forschungsaktivitäten. Es wurden deshalb per 31.12.2003 Mitarbeiter im Bereich Toolkit angestellt, wie in Abschnitt „*Organisationsstruktur*“ dargestellt.

3. Vermögensstand

3.1 Vermögensentwicklung

Die Stiftung konnte Ihren Vermögensstand im Berichtszeitraum vom ursprünglich durch das IAIK der TU Graz gewidmete

Stammvermögen von	€	2.320.000,00	auf
ein Eigenkapital von	€	2.819.147,07	per 31.12.2003 steigern

Das Eigenkapital per 31.12.2003 setzt sich zusammen aus

Stammvermögen	€	2.320.000,00
Sonstiges Vermögen (Rücklage)	€	450.000,00
Bilanzgewinn	€	49.147,07

Die Steigerung ist neben dem Zins- und Renditenertrag aus dem Stammvermögen vor allem in einer Zuwendung durch das IAIK der TU Graz in Höhe von € 450.000 begründet.

3.2 Veranlagung des Stiftungsvermögens

Es wurden im Berichtszeitraum keine Änderungen in der Veranlagung des Stammvermögens vorgenommen.

Anhang: Medienresonanz

Die folgenden Pressemeldungen sind anlässlich des „Best Paper Award“ (siehe 2.1.1) erschienen:

Sichere Markenartikel

Die Stiftung „Secure Information and Communication Technologies“ (SIC) hat erstmals einen „Best Paper Award“ für Studierende ausgeschrieben. Gewinner ist der 24-jährige, in Birkfeld in der Steiermark geborene Telematikstudent ***Martin Feldhofer*** (Foto). Er zeigt in „A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags“ wie Markenware vor unerlaubtem Kopieren geschützt werden kann. Mit der Authentifizierung von Markenartikeln durch „Radio Frequency Identification Smart Tags“, Schaltungen, die an den Artikeln angebracht sind, versucht heute vereinzelt die Bekleidungsindustrie ihre Ware zu schützen. Feldhofer entwickelte ein Protokoll, das mittels kryptografischer Algorithmen diese Authentifizierung durchführen kann. (red)

Sommerliche Professorenernennung

Der 1961 in der ehemaligen DDR geborene Chemiker Frank Uhlig wurde im Juli Professor für Anorganische Chemie an der TU Graz. Uhlig promovierte und habilitierte zum Themenfeld Organophosphane und -phosphide und und war ehe er im Sommer 2002 Gastprofessor in Graz wurde an der Universität Dortmund. Mitte der 90er hatte er ein Stipendium an der Syracuse University, New York. (red)

DER STANDARD, 28.7.2003, S. 12

■ Preisgekrönt

Die im Frühjahr an der TU Graz gegründete Stiftung zur Informationssicherheit hat nun erstmals einen Wettbewerb ausgeschrieben. Studenten wurden angeregt, Arbeiten zur Informationssicherheit zu verfassen. Dabei wurde nun der Telematik-Student **Martin Feldhofer** als Gewinner ermittelt. Er zeigte auf, wie Markenware zuverlässig vor unerlaubtem Kopieren und Fälschen geschützt werden kann.

GRAZER WOCHE, 27.7.03, S. 39

BEZIRK WEIZ

DONNERSTAG, 24. JULI 2003, SEITE 19

Martin Feldhofer aus Birkfeld bekam für seine Arbeit zur Informationssicherheit den „Best Paper Award" PATZ

Verschlüsselte Welten

Telematik-Student aus Birkfeld wurde von TU-Stiftung ausgezeichnet.

ULLA PATZ

24 Jahre alt, Telematikstudium bisher in Mindestzeit und als „bester Informatiker" von der Stiftung „SIC" der Technischen Universität Graz ausgezeichnet: das ist der Birkfelder Martin Feldhofer. Er bekam die Auszeichnung „Best Paper Award", der erstmals vergeben wurde.

Feldhofer schreibt derzeit an seiner Diplomarbeit. Auch dort beschäftigt er sich mit dem Thema „Radio Frequency Identification (RFID)". Dabei geht es darum, wie Konsumgüter mit Microchips ausgestattet werden können, um sie als Markenware zu schützen. In Ansätzen ist diese Methode schon vorhanden. Ein Bekleidungshersteller etwa näht in seine Pullis Chips ein, um die Produktwege verfolgen zu können. Ist die Entwicklung ausgereift, so könnte etwa jeder Kunde prüfen, ob das Kleidungsstück, das er kauft, auch wirklich die Marke ist, die es vorgibt zu sein.

Noch wichtiger etwa könnte diese Entwicklung bei Geldscheinen sein. Eine Blüte könnte durch einen derartigen Chip sofort erkannt werden.

Feldhofer nun erarbeitete, wie ein Datenaustausch zwischen einem Chip und einem Lesegerät erfolgen kann und wie die Daten sicher verschlüsselt und wieder entziffert werden können.

Für seine Arbeit ist Feldhofer im Dezember zu einer mehrtägigen internationalen Fachkonferenz in Las Vegas eingeladen.