stiftung secure information and communication

Jahresbericht 2014

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 2014 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 26/ Mai 2015

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 Wissens-transfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikations-technologie 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 2014 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2014 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2014 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Mit „*Cloud Computing Security*“ war die zweite von der Stiftung initiierte Stiftungs-professur 2014 in ihrem ersten vollen Jahr. Sie ist mit Prof. Mangard besetzt, die Stiftung finanzierte diese samt einer AssistentInnen-Stelle zu jeweils zwei Drittel.
- Die Personalkosten der Vorlesung „*Kritische Informationsinfrastrukturen*“ an der TU Graz wurden finanziert.
- Drei Studierenden wurde für beste Ferial-, Bakkalaureats- und Master-Arbeiten ein Best@IAIK Award gestiftet.
- Die Stiftung hat sich im EU Projekt STORK 2.0 beteiligt. Es ist dies ein Large Scale Pilot zur Interoperabilität elektronischer Identität.
- 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 2014 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 7. Mai 2015 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 vor allem über Rücklagen 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 2014 über die Stiftungsprofessur Cloud Computing, die Lehrveranstaltung kritische Informations-infrastrukturen, sowie Best Project Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Über die beiden Stiftungsprofessuren „*Kryptographie*“ und „*Cloud Computing Security*“ werden exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt. Im Berichtszeitraum 2014 war eine Nachbesetzung der Stiftungsprofessur Kryptographie noch nicht abgeschlossen, die Aktivitäten werden deshalb vor allem in der Stiftungsprofessur Cloud Computing Security berichtet.

Die Stiftung war im EU Large Scale Pilot „STORK 2.0“ engagiert. Mit „CREDENTIAL“ wurde ein weiteres EU Forschungsprojekt zugeschlagen, das 2015 starten wird.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung ist etwas (um eine Person) 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 Erträgnisse aus dem pekuniären Stamm-vermögen 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.

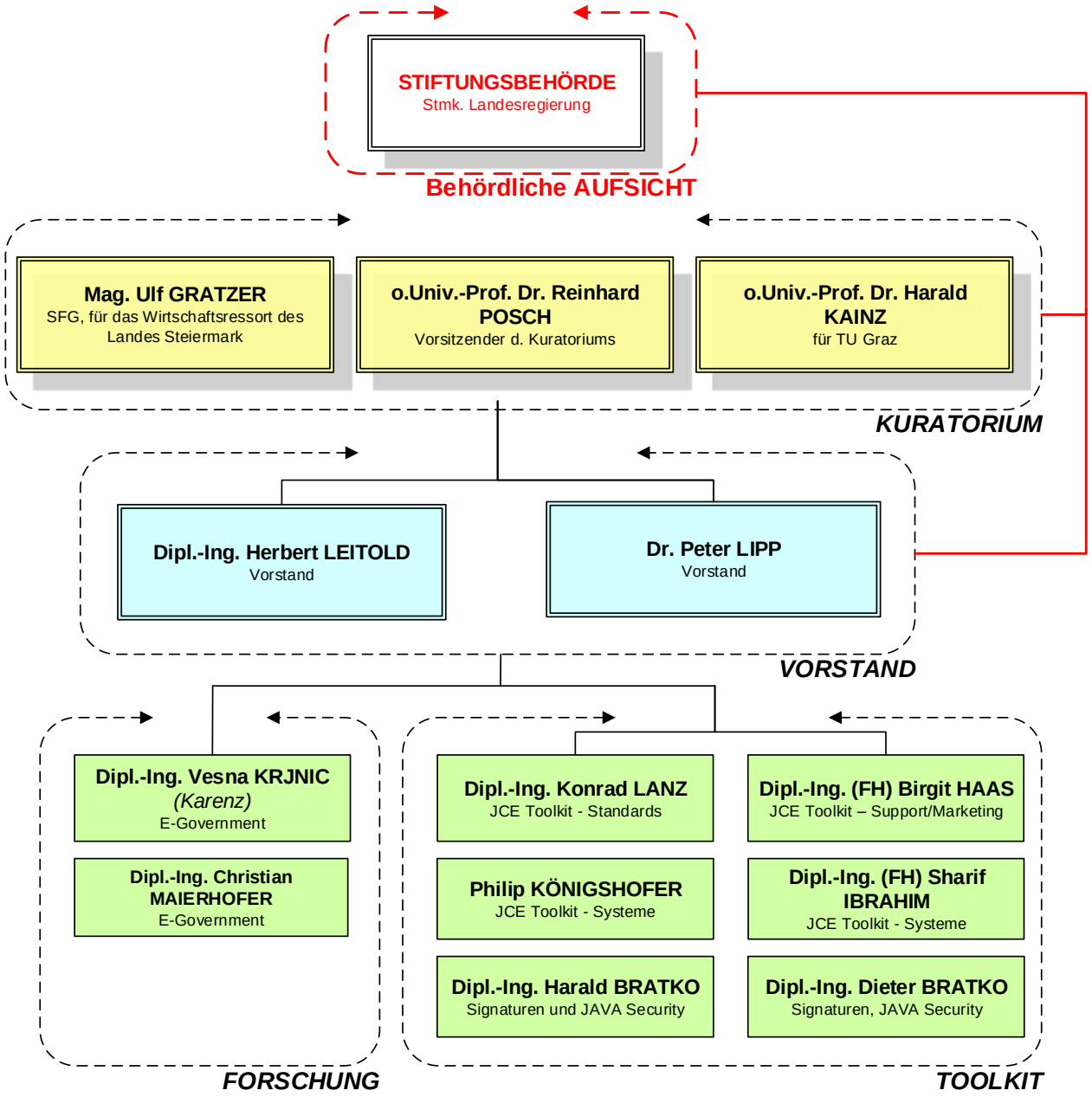
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2014 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr.techn. Dr.h.c. Harald Kainz (für die TU Graz)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
  - 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 31.12.2014 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2014

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

Diese Stiftungsprofessur wurde 2004 eingerichtet und von der Stiftung durchgängig bis 2013 co-finanziert. Nach Wechsel von Prof. Vincent Rijmen 2012 nach Leuven wurde als Überbrückung bis zur Nachbesetzung eine mit Florian Mendel besetzte Gastprofessur unterstützt. Die Nachbesetzung war 2014 im Laufen, der Abschluss wird 2015 erwartet.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, sie wird dazu mit der Nachbesetzung eine AssistentInnenstelle finanziell unterstützen.

Organisatorisch sind die aus dieser aktuell unbesetzten Professur mit Kryptographie befassten Mitarbeiterinnen und Mitarbeiter während der Nachbesetzung der neuen Professur Cloud Computing Security zugeordnet, wissenschaftliche Leistungen werden deshalb im folgenden Abschnitt berichtet.

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.

Zusammen mit der aus der Professur Informationssicherheit entstandenen Gruppe konnte im Jahr 2014 ein sehr starkes Signal in der Wissenschaft gesetzt werden. Dies zeigt sich nicht zuletzt in der hohen Zahl an Publikationen, die auch auf erstklassigen Tagungen präsentiert und in relevanten Sammelbänden veröffentlicht werden konnten:

1. Thomas Korak - "Location-dependent EM Leakage of the ATxmega Microcontroller" - The 7th International Symposium on Foundations & Practice of Security FPS'2014

2. Christoph Erwin Dobraunig, Florian Mendel, Martin Schläffer - "Differential Cryptanalysis of SipHash" - Selected Areas in Cryptography

3. Raphael Spreitzer, Jörn-Marc Schmidt - "Group-Signature Schemes on Constrained Devices: The Gap Between Theory and Practice" - CS2'14 Proceedings

4. Raphael Spreitzer, Benoit Gérard - "Towards More Practical Time-Driven Cache Attacks" - Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014. Proceedings.

5. Christoph Erwin Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel - "On the Security of Fresh Re-Keying to Counteract Side-Channel and Fault Attacks" - Smart Card Research and Advanced Applications

6. Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, Martin Schläffer - "Malicious Hashing: Eve's Variant of SHA-1" - Selected Areas in Cryptography

7. Zhe Liu, Erich Wenger, Johann Großschädl - "MoTE-ECC: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks" - Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings

8. Andrey Bogdanov, Christoph Erwin Dobraunig, Maria Eichlseder, Martin Lauridsen, Florian Mendel, Martin Schläffer, Elmar Tischhauser - "Key Recovery Attacks on Recent Authenticated Ciphers" - Progress in Cryptology - LATINCRYPT 2014

9. Thomas Korak, Michael Hutter, Baris Ege, Lejla Batina - "Clock Glitch Attacks in the Presence of Heating" - Workshop on Fault Diagnosis and Tolerance in Cryptography - FDTC 2014, Busan, Korea, September 23, 2014, Proceedings

10. Thomas Korak, Thomas Plos - "EM Leakage of RFID Devices - Comparison of Two Measurement Approaches" - The 9th International Conference on Availability, Reliability and Security (ARES 2014)

11. Maria Eichlseder, Florian Mendel, Martin Schläffer - "Branching Heuristics in Differential Collision Search with Applications to SHA-512" - Fast Software Encryption

12. Raphael Spreitzer - "PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices" - 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)

13. Hannes Groß, Erich Wenger, Honorio Martín, Michael Hutter - "PIONEER - a Prototype for the Internet of Things based on an Extendable EPC Gen2 RFID Tag" - Workshop on RFID Security - RFIDsec 2014, 10th Workshop, Oxford, UK, July 21 -23, 2014, Proceedings.

14. Erich Wenger, Paul Wolfger - "Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster" - Selected Areas in Cryptography - SAC 2014

15. Florian Mendel, Vincent Rijmen, Martin Schläffer - "Collision Attack on 5 Rounds of Grøstl" - Fast Software Encryption

16. Thomas Korak, Michael Hutter - "On the Power of Active Relay Attacks using Custom-Made Proxies" - 2014 IEEE International Conference on RFID (IEEE RFID) (IEEE RFID 2014)

17. Thomas Korak, Michael Höfler - "On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms" - 11th Workshop on Fault Diagnosis and Tolerance in Cryptography

18. Thomas Unterluggauer, Erich Wenger - "Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices" - Ninth International Conference on Availability, Reliability and Security (ARES), 2014

19. Thomas Unterluggauer, Erich Wenger - "Efficient Pairings and ECC for Embedded Systems" - Cryptographic Hardware and Embedded Systems - CHES

2014, 16th International Workshop, Busan, Korea, September 23 - September 26, 2014, Proceedings.

20. Robert Schilling, Manuel Jelinek, Markus Ortoff, Thomas Unterluggauer - "A Low-area ASIC Implementation of AEGIS128, a Fast Authenticated Encryption Algorithm" - 22nd Austrian Workshop on Microelectronics (Austrochip)

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*Einführung in die Informationssicherheit*“, „*Applied Cryptography*“ und „*Applied Cryptography 2*“, „*IT Security*“, „*System on Chip*“ und „*VLSI Design*“ betreut. Das Angebot wird mit Seminaren, Bakkalaureats- und Master-Arbeiten, sowie Dissertationsbetreuungen ergänzt.

Die von der Stiftung mit-finanzierte Professur ist also Quelle erstklassischer Forschung im Bereich der Kryptographie und Informationssicherheit. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die internationales Ansehen genießt.

2.1.3 Best Project Award

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2014 wurden Preise an drei Studierende der TU Graz vergeben:

1. Beste Ferialarbeit: Michael Rodler für die Arbeit „Security of Mobile Applications“
2. Beste Bakkalaureats-Arbeit: Simone Griesmayr für die Arbeit „Fingerprinting Websites on Android Smartphones“
3. Beste Masterarbeit: Florian Achleitner für die Arbeit „A Secure-World Managed Runtime for ARM TrustZone“

Die prämierten Studierenden erhielten Gutscheine für die Teilnahme an Konferenzen oder Sommerschulen bzw. eine Smart Watch.

2.1.4 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 elektronischer 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.

2.1.5 Vorlesung Kritische Informationsinfrastrukturen

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

2.1.6 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.

2.1.7 Eigene Forschungsleistungen

Mitarbeiter der Stiftung haben eigenständige Forschung im Bereich elektronischer Identität und Signaturen insbesondere in Cloud Umgebungen durchgeführt. Es wurden daraus Forschungsprojekte definiert und zusammen mit anderen Forschungsgruppen zur weiteren Förderung eingereicht. Dabei hat das Projekt „CREDENTIAL“ im hoch kompetitiven EU Förderprogramm Horizon 2020 den Zuschlag erhalten. Das Projekt wird 2015 starten.

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 2014 sehr gut. Dies wurde über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen ergänzt.