Jahresbericht 2022

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

Auskünfte

Stiftung Secure Information and Communication Technologies SIC
Inffeldgasse 16a
8010 Graz
Tel.: (0316) 873-5552 / 5576 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. Harald Bratko, Dr. Thomas Zefferer (Vorstand der Stiftung)

Graz, am 23. Mai 2023

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 2022 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 01.01.2022 – 31.12.2022 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2022 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Zur Professur „Kryptographie" von Prof. Christian Rechberger wurde bis August 2022 eine AssistentInnenstelle zu zwei Drittel finanziert.
- 12 Studierende wurden mit einem Research Excellence Award ausgezeichnet.
- 2 Studierende wurden im Rahmen des TU Graz 100 Stipendienprogramms gefördert.
- Die Stiftung ist Partner im EU Forschungsprojekt KRAKEN.
- Der Hilfsbetrieb JCE Toolkit hat wiederum Gewinne erwirtschaftet, die dem gemeinnützigen Forschungsbereich zufließen.

Inhaltsverzeichnis

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 2022 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 11. Mai 2023 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 (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 Informationssicherheit.*
>
> *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 https://jce.iaik.tugraz.at/about-us/ 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 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 oben genannten 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 2022 über die Stiftungsprofessur „Kryptographie“, sowie Research Excellence Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Über die Stiftungsprofessur „Kryptographie“ werden bzw. wurden exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt.

Die Stiftung nahm am EU Projekt „KRAKEN“ teil, das Ende 2019 gestartet ist, womit sie auch in internationalen Forschungsaktivitäten verankert ist.

Der Hilfsbetrieb „JCE Toolkit“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand ist um eine Person gestiegen.

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 abgabenrechtlichem 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

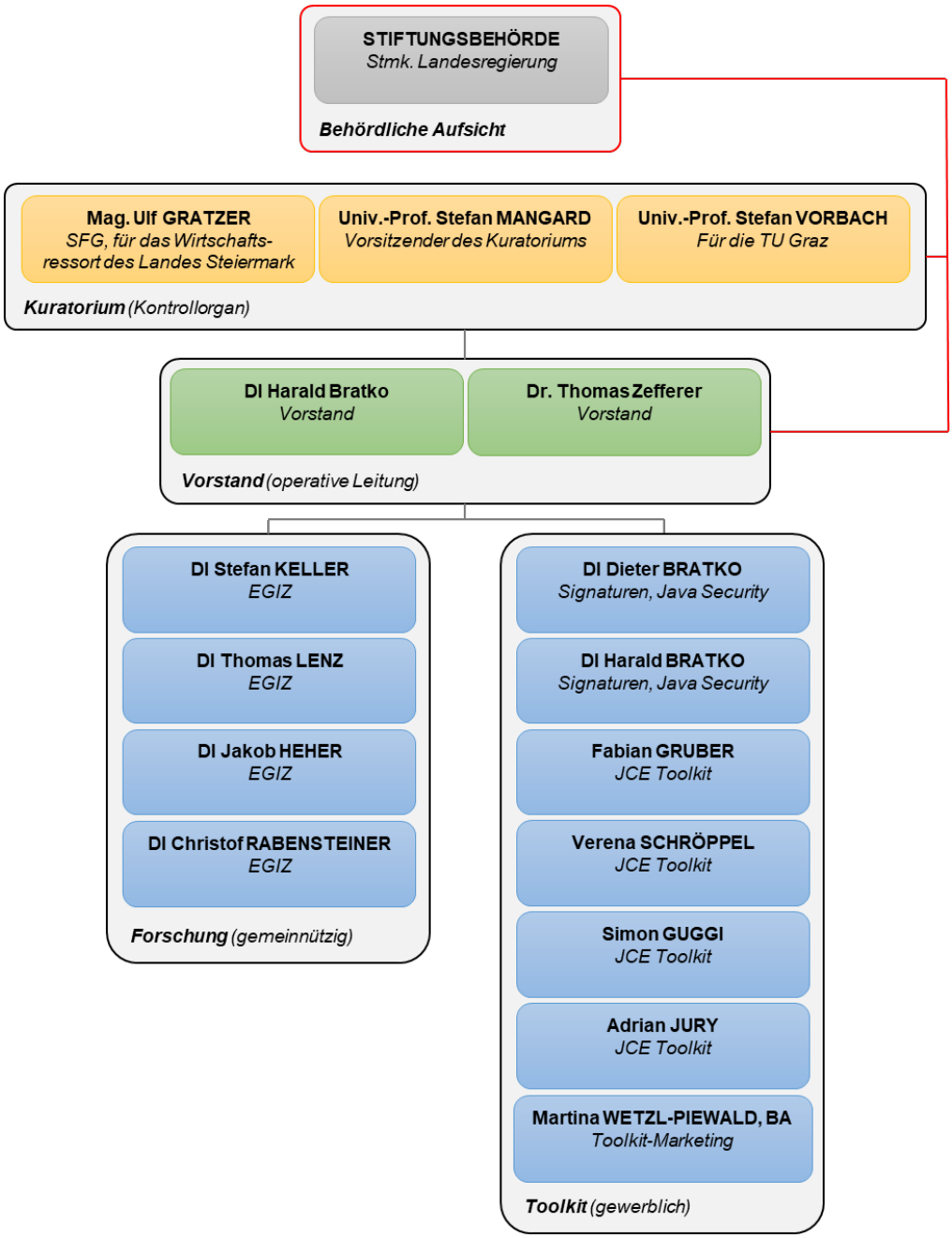
Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2022 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - Univ.-Prof. Dr. Stefan Vorbach (für die TU Graz)
    - Univ.-Prof. Dr. Stefan Mangard (Vorsitzender Kuratorium)
  - Staatliche Aufsicht ist Stiftungsbehörde der Steiermärkischen Landesregierung, Abteilung 3 Verfassung und Inneres; Referat Personenstand, Veranstaltung, Innerer Dienst; Bundesstiftungen und -Fonds / Landesstiftungen und -Fonds
- Die Führungsebene bildet der Vorstand
  - Dipl.-Ing. Herbert Leitold (bis 30.06.2022)
  - Dipl.-Ing. Harald Bratko (ab 01.07.2022)
  - Dr. Thomas Zefferer
- 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 nichtkommerziellen Forschung kostenlos verwendbare Werkzeuge.

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Stand an Mitarbeiterinnen und Mitarbeitern der Stiftung per 31.12.2022 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2022

2. Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird nach dem in der Satzung der Stiftung definierten Zweck „Förderung von Forschung und Lehre“ berichtet.

2.1. Förderung von Forschung und Lehre, Wissenstransfer

2.1.1. Stiftungsprofessur Kryptographie

Diese Stiftungsprofessur wurde 2004 eingerichtet und von der Stiftung durchgängig kofinanziert. Nach Wechsel von Prof. Vincent Rijmen 2012 nach Leuven wurde als Überbrückung eine Gastprofessur von Florian Mendel finanziert. Seit 2017 ist die Professur mit Prof. Christian Rechberger besetzt. Die Stiftung hat 2017 eine vorgezogene Bestellung mit einer Überbrückungsfinanzierung unterstützt.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, es bestand eine Finanzierungszusage einer AssistentInnenstelle. Diese wurde Mitte 2017 besetzt und lief im August 2022 aus. Derzeit wird die Finanzierung einer weiteren Stelle geprüft.

Die Gruppe um Prof. Rechberger konnte 2022 ihre Ergebnisse an namhaften und auch erstklassigen wissenschaftlichen Tagungen und Journalen veröffentlichen. Eine Auswahl an solchen Veröffentlichungen ist in Folge gegeben und soll zeigen, dass sich aus der von der Stiftung zusammen mit der TU Graz initiierten Professur eine Gruppe entwickelt hat, die erstklassige wissenschaftliche Forschung in der Steiermark betreibt:

- Bampoulidis, A., Bruni, A., Helminger, L., Kales, D., Rechberger, C. & Walch, R.: “Privately Connecting Mobility to Infectious Diseases via Applied Cryptography”, In: Proceedings on Privacy Enhancing Technologies 2022. Vol. 4. p. 768-788 34 p.
- Grassi, L., Khovratovich, D., Rønjom, S. & Schofnegger: “The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over (F_p)^n”, In: IACR Transactions on Symmetric Cryptology. 2022, 1, p. 5-37 33 p.
- Cid, C., Grassi, L., Gunsing, A., Lüftenegger, R., Rechberger, C. & Schofnegger: “Influence of the Linear Layer on the Algebraic Degree in SP-Networks”, In: IACR Transactions on Symmetric Cryptology. 2022, 1, p. 110-137 28 p.
- Lüftenegger, R., Rechberger, C., Grassi, L., Schofnegger, M., Walch, R. & Khovratovich: “Reinforced Concrete: A Fast Hash Function for Verifiable Computation”, In: CCS 2022 - Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Association of Computing Machinery, p. 1323–1335 13 p.
- CryptoDobraunig, C. E., Kales, D., Rechberger, C., Schofnegger, M. & Zaverucha: “Shorter Signatures Based on Tailor-Made Minimalist Symmetric-Key”, In: CCS 2022 - Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Association of Computing Machinery, p. 843–857 15 p.
- Helminger, L. & Rechberger, C.: Multi-Party Computation in the GDPR, In: Privacy Symposium 2022 - Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT).

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*IT Sicherheit*“, „*Cryptography*“, „*Applied Cryptography*“ und „*Applied Cryptography 2*“ gehalten, wie auch Seminare, Bakkalaureats- und Master-Arbeiten, sowie Dissertationen betreut werden.

2.1.2. Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2022 wurden Preise an zwölf Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- **Simone Franza** und **Markus Köstl** für „*SQUIP: Exploiting the Scheduler Queue Contention Side Channel*“ eingereicht und akzeptiert bei der Konferenz IEEE S&P 2023
- **Lukas Lamster** für „*CSI:Rowhammer - Cryptographic Security and Integrity against Rowhammer*“ eingereicht und akzeptiert bei der Konferenz IEEE S&P 2023
- **Stefan Pranger** für “*Automata Learning meets Shielding*” eingereicht und akzeptiert bei der Konferenz ISOLA 2022
- **Alexander Palmisano** für „*Online Shielding for Reinforcement Learning*“ eingereicht und akzeptiert bei der Konferenz ISSE 2022
- **Andreas Kogler** für „*PLATYPUS: Software-based Power Side-Channel Attacks on x86*“ eingereicht und akzeptiert bei der Konferenz IEEE S&P 2021
- **Jonas Juffinger** für „*Half-Double: Hammering From the Next Row Over*“ eingereicht und akzeptiert bei der Konferenz USENIX Security 2022
- **Thomas Schuster** für „*Robust and Scalable Process Isolation against Spectre in the Cloud*“ eingereicht und akzeptiert bei der Konferenz ESORICS 2022
- **Amel Smajic** für „*Systematic Analysis of Programming Languages and Their Execution Environments for Spectre Attacks*“ eingereicht und akzeptiert bei der Konferenz ICISSP 2022
- **Erik Kraft** für „*Remote Memory-Deduplication Attacks*“ eingereicht und akzeptiert bei der Konferenz NDSS 2022
- **Martin Haubenwallner** für „*Finding and Exploiting CPU Features using MSR Templating*“ eingereicht und akzeptiert bei der Konferenz IEEE S&P 2022
- **Johannes Erlacher** für „*Bounds for the Security of Ascon against Differential and Linear Cryptanalysis*“ eingereicht und akzeptiert bei der Konferenz ToSC 2022/1

Die prämierten Studierenden erhielten jeweils Graz-Gutscheine im Wert von € 200. In Summe wurde somit € 2.400,00 an Gutscheinen zur Verfügung gestellt.

2.1.3. TU Graz 100 Stipendien

Im Rahmen des von der TU Graz ins Leben gerufenen Stipendienprogramms „TU Graz 200“ fördert die Stiftung SIC 2 Studierende über Stipendien, die diese während ihres Master-Studiums an der TU Graz beziehen. Folgende Studierende werden durch die Stiftung SIC über Stipendien finanziell unterstützt:

- Carina Fiedler (Master-Studium „Computer Science“)
- Ernesto Martinez Garcia (Master-Studium „Computer Science“)

Die erste Tranche des Stipendiums (in Summe € 4.000,00) wurde im Wintersemester 2022/23 an die beiden Studierenden überwiesen.

2.1.4. KRAKEN

Als EU-Forschungsprojekt mit Beteiligung der Stiftung ist im Dezember 2019 das Projekt KRAKEN (broKeRage And marKEt platform for persoNal data) gestartet. Ziel dieses Projekts mit zehn Partnern in sechs Ländern war es, Lösungen zu datenschutzkonformem Teilen personenbezogener Daten unter Kontrolle der Betroffenen zu erforschen.

2.1.5. E-Government

Mitarbeiter des Bereichs Forschung der Stiftung unterstützen das E-Government Innovationszentrum (EGIZ). EGIZ ist eine Initiative des Bundesministeriums für Digitalisierung und Wirtschaftsstandort und der TU Graz zur wissenschaftlichen Weiterentwicklung des E-Government in Österreich, seit 2020 ist EGIZ in das Zentrum für sichere Informationstechnologie - Austria (A-SIT) eingebunden. Experten der Stiftung werden zu Projekten beigezogen.

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 hinaus wurde bis auf eine Software-Lizenz 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 2022 im Schnitt der letzten Jahre. Dies wurde über Aufträge zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdienstanbieter ergänzt.