Jahresbericht 2023

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 29. Mai 2024

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 2023 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 01.01.2023 – 31.12.2023 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2023 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- 4 Studierende wurden mit einem Research Excellence Award ausgezeichnet.
- 2 Studierende wurden im Rahmen des TU Graz 100 Stipendienprogramms gefördert.
- Die Stiftung unterstützte den Austrian Computer Science Day 2023.
- Die Stiftung hatte Forschungsaktivitäten im Bereich E-Government.
- Die Stiftung ist Partner im KIRAS Forschungsprojekt PREPARED.
- 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 2023 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://sic.tech/about-us/ 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 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 eines über mehrere Jahre anhaltenden geringen Zinsniveaus und einer in den letzten Jahren schwierigen Situation im Wertpapier-Bereich 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 2023 über die Research Excellence Awards und die Finanzierung von Stipendien im Rahmen des TU Graz 100 Stipendien-Programms vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Die Stiftung unterstützte außerdem den an der TU Graz abgehaltenen Austrian Computer Science Day 2023, wodurch entsprechend der Satzung der Stiftung die wissenschaftliche Forschung und der Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit unterstützt wurde.

Die Stiftung nimmt außerdem am KIRAS Projekt „PREPARED“ teil, das Ende 2023 gestartet ist, womit sie auch in Forschungsaktivitäten verankert ist.

Der Hilfsbetrieb „JCE Toolkit“ konnte auch 2023 einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand ist mit Stand 31.12.2023 im Vergleich zum Vorjahr (31.12.2022) 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 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.

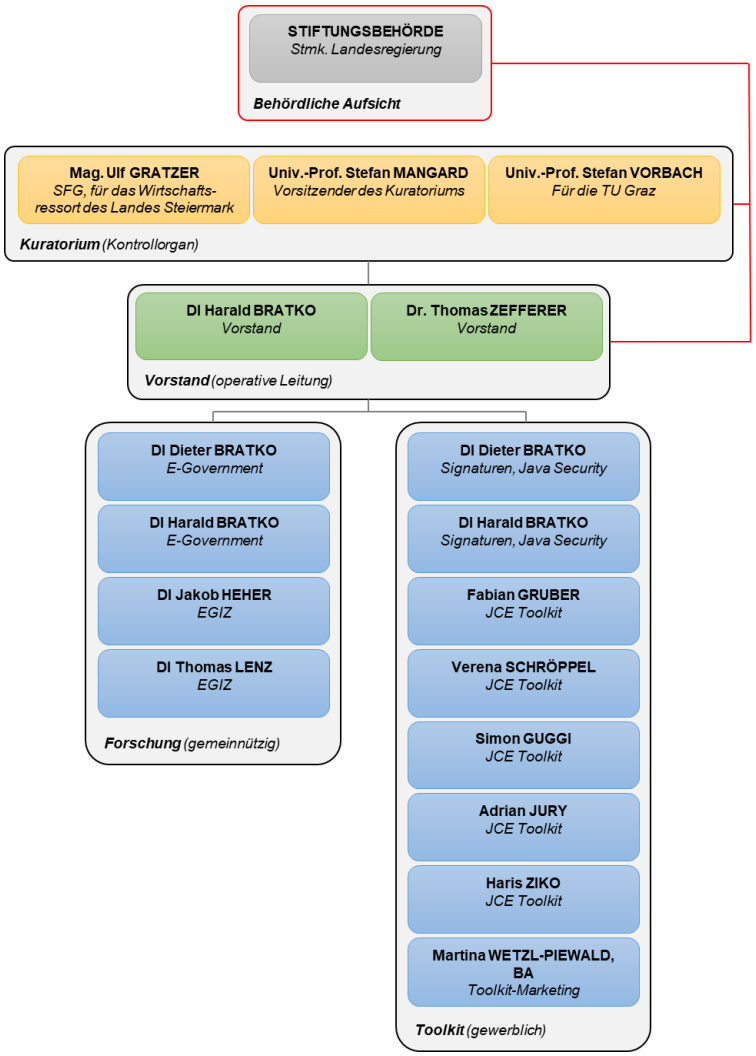
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2023 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 die 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. Harald Bratko
  - Dr. Thomas Zefferer
- Die operative Ebene wird durch zwei Säulen gebildet:
  - Der Bereich *Forschung* umfasst die mit eigenständiger Durchführung von Forschung und Entwicklung befassten Mitarbeiter:innen 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 Mitarbeiter:innen der Stiftung per 31.12.2023 dargestellt. Herr DI Dieter Bratko und Herr DI Harald Bratko waren 2023 sowohl im Bereich Forschung als auch im Bereich Toolkit tätig. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2023

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

Eine im Jahr 2004 eingerichtete Stiftungsprofessur bzw. die Finanzierung einer Assistent:innenstelle ist im August 2022 ausgelaufen. Der Bedarf an der Finanzierung einer weiteren Stelle wird laufend evaluiert. Da ein solcher Bedarf derzeit nicht gegeben ist, wird das Augenmerk aktuell – wie im Folgenden ausgeführt – verstärkt auf die Unterstützung von Studierenden (Awards, Stipendien, etc.) bzw. auch auf die Unterstützung von Veranstaltungen im Stiftungszweck und eigene Forschungsaktivitäten gelegt.

2.1.1. Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2023 wurden Preise an vier Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- **Moritz Waser** für „*SPEAR-V: Secure and Practical Enclave Architecture for RISC-V*“ eingereicht und akzeptiert bei der Konferenz ASIA CCS `23
- **Felix Pallua** für „*Finding Collisions for Round-Reduced Romulus-H*“ eingereicht und akzeptiert bei der Konferenz ToSC 2023/1
- **Esma Galijatović** für „*Integrity of Virtual Testing for Crash Protection*“ eingereicht und akzeptiert für das Journal Frontiers in Future Transportation
- **Alexander Plamisano** für „*Safety Shielding under Delayed Observation*“ eingereicht und akzeptiert bei der Konferenz ICAPS 2023

Die prämierten Studierenden erhielten jeweils Graz-Gutscheine im Wert von € 200,00. In Summe wurde somit € 800,00 an Gutscheinen zur Verfügung gestellt.

2.1.2. TU Graz 100 Stipendien

Im Rahmen des von der TU Graz ins Leben gerufenen Stipendienprogramms „TU Graz 100“ fördert die Stiftung SIC zwei 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“)

Nachdem die erste Tranche des Stipendiums (in Summe € 4.000,00) bereits im Wintersemester 2022/23 an die beiden Studierenden überwiesen wurde, wurden im Sommersemester 2023 und im Wintersemester 2023/2024 nach Prüfung des Studienerfolgs weitere Tranchen des Stipendiums ausbezahlt. Im Summe wurden im Jahr 2023 damit € 8.000,00 an die beiden Studierenden ausbezahlt.

2.1.3. Austrian Computer Science Day 2023

Der Austrian Computer Science Day (ACSD) ist eine jährliche Veranstaltung, die Informatiker aus ganz Österreich und darüber hinaus zusammenbringt, um die Sichtbarkeit des Fachgebiets zu verbessern und die Zusammenarbeit in Forschung und Lehre zu fördern. Im Jahr 2023 fand der ASCD an der Technischen Universität Graz statt. Die Stiftung unterstützte die Organisation und Durchführung der Veranstaltung finanziell mit einem Betrag von € 3.000,00.

2.1.4. Forschung im Bereich E-Government

Mitarbeiter:innen 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.

2.1.5. Forschung im Bereich Post-Quanten-Kryptographie

Elektronische Signaturen stellen die technische Basis aktueller E-Government-Lösungen dar. Dabei ist zu beachten, dass aktuell in der Praxis eingesetzte Verfahren durch Angriffe mit leistungsstarken Quantencomputern bedroht sind. Aus diesem Grund wurde durch das US-amerikanische National Institute of Standards and Technology (NIST) ein Standardisierungsprozess für post-quanten-sichere Verfahren zur Substituierung bisheriger Signaturverfahren gestartet. Ergebnisse aus diesem NIST-Prozess ermöglichen es nun, Systeme für die Migration auf Post-Quanten-Kryptographie vorzubereiten. Jedoch fehlen bis dato in vielen Bereichen praktische Erfahrungen für einen solchen Migrationsprozess. Das KIRAS Projekt PREPARED verfolgt deshalb das Ziel, post-quanten-sichere Signaturverfahren speziell im Kontext von eID-Systemen zu analysieren. Insbesondere wird ein Migrationsplan entwickelt, da gerade Systeme mit langlebigen Zertifikaten und Signaturen eine entsprechende Vorbereitung benötigen, um eine Migration rechtzeitig und problemlos durchführen zu können. Die Stiftung SIC ist Partner im KIRAS Projekt PREPARED und bringt ihre Expertise zur Implementierung kryptographischer Algorithmen in das Projekt ein.

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 2023 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 2023 – hauptsächlich bedingt durch eine inflationsbedingt notwendige Preiserhöhung – etwas über dem Schnitt der letzten Jahre. Dies wurde über Aufträge zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdienstanbieter ergänzt.