Jahresbericht 2025

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

Auskünfte

Stiftung Secure Information and Communication Technologies SIC
Sandgasse 38a
8010 Graz
Tel.: (0316) 873-5552 / 5576 Fax.: (0316) 873-5520

Impressum

Medieninhaber, Herausgeber und Verleger
Stiftung Secure Information and Communication Technologies SIC, Sandgasse 38a, 8010 Graz

Redaktion und für den Inhalt verantwortlich
Dipl.-Ing. Harald Bratko, Dr. Thomas Zefferer (Vorstand der Stiftung)

Graz, am 11. Juni 2026

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 2025 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 01.01.2025 – 31.12.2025 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2025 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- 15 Studierende wurden mit einem Student Research Excellence Award ausgezeichnet.
- 8 Studierende wurden mit einem ISEC Bachelor Excellence Award ausgezeichnet.
- Die Stiftung unterstützte die Konferenz DIMVA 2025.
- Die Stiftung unterstützte die Konferenz LogicLounge 2025.
- Die Stiftung hatte Forschungsaktivitäten im Bereich E-Government.
- Die Stiftung war Partner im KIRAS Forschungsprojekt PREPARED.
- Die Stiftung ist Partner im Horizon Europe Forschungsprojekt POSEIDON.
- 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)[1] 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 2025 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

[1] Im Jahr 2025 erfolgte eine Umbenennung des Instituts in *Institute of Information Security (ISEC)*.

- 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 schwankenden 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 muss.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2025 insbesondere über die Research Excellence Awards und ISEC Bachelor Excellence Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Die Stiftung unterstützte außerdem die Organisation und Durchführung der Veranstaltungen DIMVA 2025 und LogicLounge 2025, die vom ISEC der TU Graz organisiert wurden. Dadurch wurde entsprechend der Satzung der Stiftung die wissenschaftliche Forschung und der Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit unterstützt.

Die Stiftung nahm außerdem am KIRAS Projekt „PREPARED“ teil, das Ende 2023 gestartet ist, womit sie auch in Forschungsaktivitäten verankert war. Das Projekt endete nach kostenneutraler Verlängerung im Jänner 2026.

Seit Oktober 2025 nimmt die Stiftung zudem am Horizon Europe Forschungsprojekt POSEIDON teil und setzt so eigene Forschung im Bereich postquantenresistenter kryptographischer Algorithmen auf europäischer Ebene fort. Hier erfolgt eine enge Zusammenarbeit mit dem ISEC der TU Graz, das in diesem Forschungsprojekt ebenfalls Partner ist.

Der Hilfsbetrieb „Toolkit“ konnte auch 2025 einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt.

Der Personalstand ist mit Stand 31.12.2025 im Vergleich zum Vorjahr (31.12.2024) um zwei Personen 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 (seit 2025 nach erfolgter Umbenennung ISEC) 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).

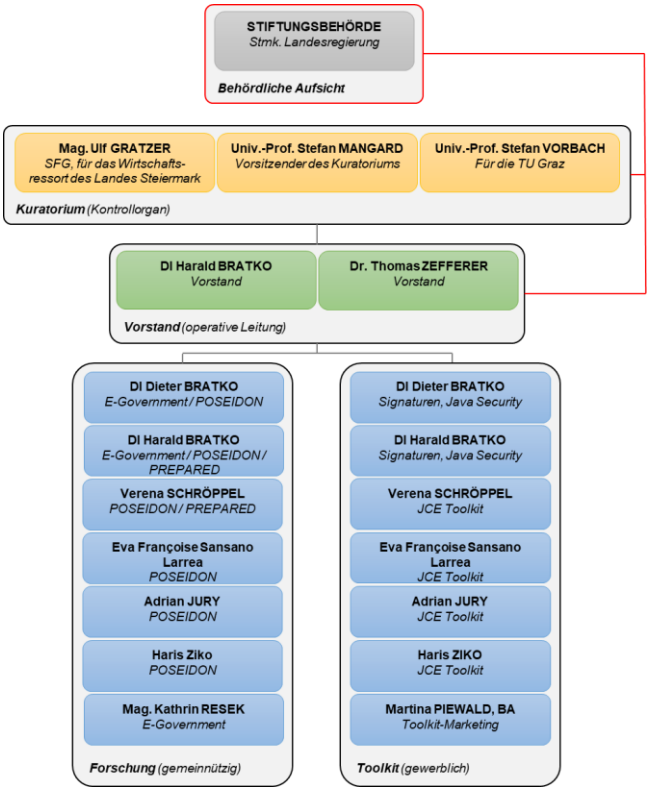
1.5. Stiftungsorgane und Organisationsstruktur

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 2025 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 31.12.2025 dargestellt. Frau Schröppel, Frau Eva Françoise Sansano Larrea, Herr DI

Dieter Bratko und Herr DI Harald Bratko waren 2025 sowohl im Bereich Forschung als auch im Bereich Toolkit tätig. Administration und technische Infrastruktur wird gegen Kostenersatz vom ISEC der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2025

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. Student Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2025 wurden Preise an 15 Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- **Lukas Schwarz** für *„Presshammer: Rowhammer and Rowpress without Physical Address Information“* eingereicht und akzeptiert bei der Konferenz DIMVA 2024
- **Lorenz Schmid** für *„Preimage-type Attacks for Reduced Ascon-Hash: Application to Ed25519“* eingereicht und akzeptiert bei der Konferenz SAC 2025
- **Marlene Jüttler** für *„AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions“* eingereicht und akzeptiert bei der Konferenz FSE 2025
- **Simon Scherer** für *„Code Encryption with Intel TME-MK for Control-Flow Enforcement“* eingereicht und akzeptiert bei der Konferenz ESORICS 2025
- **Dmytro Shvets** für *„Future-Proof Asynchronous IoT Backups: An Evaluation of Secure IoT Data Recovery Considering Post-Quantum Threats“* eingereicht und akzeptiert bei der Konferenz IFIP SEC 2025
- **Thomas Buchsteiner** für *„webSPDZ - Versatile MPC on the Web“* eingereicht und akzeptiert bei der Konferenz CANS 2025
- **Daniel Sanz Sobrino** für *„Pasta on Edge: Cryptoprocessor for Hybrid Homomorphic Encryption“* eingereicht und akzeptiert bei der Konferenz DATE 2025
- **Constantin Piber** für *„Accelerating Hash-Based Polynomial Commitment Schemes with Linear Prover Time“* eingereicht und akzeptiert bei der Konferenz TCHES 2025
- **Nora Puntigam** für *„Zero-Click SnailLoad: From Minimal to No User Interaction“* eingereicht und akzeptiert bei der Konferenz ESORICS 2025
- **Simone Franza** für *„Zero-Click SnailLoad: From Minimal to No User Interaction“* eingereicht und akzeptiert bei der Konferenz ESORICS 2025
- **Sudheendra Raghav Neela** für *„Not So Secure TSC“* eingereicht und akzeptiert bei der Konferenz ACNS 2025

- **Sebastian Daniel Felix** für „*Real-World Study of the Security of Educational Test Systems*“ eingereicht und akzeptiert bei der Konferenz OSVS (Euro S&P Workshop) 2025
- **Felix Windisch** für „*Synthesis of Controllers for Continuous Blackbox Systems*“ eingereicht und akzeptiert bei der Konferenz VMCAI 2025
- **Aaron Giner** für „*Fast and Efficient Secure L1 Caches for SMT*“ eingereicht und akzeptiert bei der Konferenz ARES 2025
- **Paul Gollob** für „*Fast and Efficient Secure L1 Caches for SMT*“ eingereicht und akzeptiert bei der Konferenz ARES 2025

Die prämierten Studierenden erhielten jeweils Graz-Gutscheine im Wert von € 200,00. In Summe wurden somit **€ 3.000,00** an Gutscheinen zur Verfügung gestellt.

2.1.2. ISEC Bachelor Excellence Award

Die Stiftung SIC unterstützt den ISEC Bachelor Excellence Award, über den vielversprechende Studierende im Bereich IT-Security nach Nachweis des entsprechenden Studienerfolgs finanziell gefördert werden. Im Jahr 2025 wurde der ISEC Bachelor Excellence Award (je € 1.000,00) an acht Studierenden ausbezahlt. In Summe wurden im Jahr 2025 damit **€ 8.000,00** im Rahmen des ISEC Bachelor Excellence Award zuerkannt und ausbezahlt.

2.1.3. DIMVA 2025

Die DIMVA (Conference on Detection of Intrusions and Malware & Vulnerability Assessment) zählt zu den etablierten internationalen Fachkonferenzen im Bereich IT-Sicherheit und fokussiert sich auf Themen wie Intrusion Detection, Malwareanalyse und Schwachstellenforschung. Die DIMVA 2025 fand von 9. bis 11. Juli 2025 an der Technischen Universität Graz statt und brachte internationale Forscher:innen aus Wissenschaft, Industrie und Behörden zusammen. Die TU Graz spielte dabei eine zentrale Rolle als Gastgeberin und organisatorischer Austragungsort der Konferenz. Forschende der TU Graz waren sowohl im Organisationskomitee als auch im wissenschaftlichen Programm vertreten und präsentierten mehrere aktuelle Forschungsarbeiten im Bereich Systemsicherheit und Side-Channel-Angriffe. Die Stiftung förderte die Organisation und Durchführung der Konferenz mit insgesamt **€ 2.000,00**.

2.1.4. LogicLounge 2025

Die LogicLounge ist ein internationales Diskussionsformat zu Themen der Logik, künstlichen Intelligenz, Informatik und Philosophie im Kontext der IT-Sicherheit und bringt renommierte Wissenschaftler:innen mit einer breiteren Öffentlichkeit zusammen. Die Veranstaltungsreihe wurde ursprünglich im Rahmen der Vienna Summer of Logic gegründet und im Jahr 2025 von der TU Graz organisiert. Die Stiftung Die Stiftung unterstützte die Organisation der Konferenz mit insgesamt **€ 3.068,36**.

2.1.5. 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.

2.1.6. 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 in Zukunft 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 verfolgte deshalb das Ziel, post-quanten-sichere Signaturverfahren speziell im Kontext von eID-Systemen zu analysieren. Insbesondere wurde 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 war Partner im KIRAS Projekt PREPARED und brachte ihre Expertise zur Implementierung kryptographischer Algorithmen in das Projekt ein. Das Projekt endete nach kostenneutraler Verlängerung im Jänner 2026.

Seit Oktober 2025 ist die Stiftung als Partner im EU Horizon Europe Projekt POSEIDON („POst-quantum SEcure dIgital iDentities for EurOpean solutioNs“) beteiligt. Das Projekt beschäftigt sich mit der Entwicklung und Erprobung von post-quanten-sicheren Kryptographieverfahren für digitale Identitäten und Vertrauensdienste in Europa. Ziel des Projekts ist es, bestehende kryptographische Verfahren schrittweise durch Post-Quanten-Kryptographie (PQC) und hybride Ansätze zu ergänzen bzw. zu ersetzen, um europäische digitale Infrastrukturen langfristig gegen zukünftige Angriffe durch Quantencomputer abzusichern. Dabei werden insbesondere Anwendungen im Bereich der European Digital Identity Wallet, Self-Sovereign Identity sowie sichere elektronische Signaturen und Authentifizierungsverfahren adressiert. Die Stiftung bringt insbesondere ihre Erfahrung in der Implementierung kryptographischer Algorithmen ein und erweitert ihre Krypto-Bibliotheken um postquantensichere Varianten.

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 ISEC (vormals IAIK) der TU Graz getragen. Darüber hinaus wurde bis auf kleinere Software-Lizenzen für Tätigkeiten im Bereich Toolkit 2024 keine Infrastruktur angeschafft, da hier die qualitativ hochwertigen Ressourcen des ISEC die Anschaffung eigener teurer Anlagen nicht rechtfertigt. Die Nutzung der Infrastruktur wird an das ISEC abgegolten.

2.2.2. Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2025 etwas über dem Schnitt der letzten Jahre. Dies wurde über Aufträge zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdienstanbieter ergänzt.