



Jahresbericht 2024

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 17. Juni 2025

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 2024 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 01.01.2024 – 31.12.2024 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2024 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- 15 Studierende wurden mit einem Research Excellence Award ausgezeichnet.
- 2 Studierende wurden im Rahmen des TU Graz 100 Stipendienprogramms gefördert.
- 4 Studierende wurden mit einem IAIK Bachelor Excellence Award ausgezeichnet.
- Die Stiftung unterstützte die Graz Security Week 2024.
- 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

Executive Summary	2
1. Einleitung.....	4
1.1. Stiftungszweck.....	4
1.2. Forschungsschwerpunkte.....	4
1.3. Zur Lage der Stiftung	5
1.4. Hilfsbetrieb JCE Toolkit.....	5
1.5. Stiftungsorgane und Organisationsstruktur	6
2. Leistungen im Sinne des Stiftungszwecks	8
2.1. Förderung von Forschung und Lehre, Wissenstransfer	8
2.1.1. Research Excellence Awards	8
2.1.2. IAIK Bachelor Excellence Award	9
2.1.3. TU Graz 100 Stipendien	9
2.1.4. Graz Security Week 2024	9
2.1.5. Forschung im Bereich E-Government.....	10
2.1.6. Forschung im Bereich Post-Quanten-Kryptographie	10
2.2. Organisatorisches und Sonstiges.....	10
2.2.1. Technische Infrastruktur	10
2.2.2. Entwicklungsaktivitäten JCE Toolkit	10

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 2024 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 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 muss.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2024 über die Research Excellence Awards, IAIK Bachelor 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 die an der TU Graz abgehaltene Summer School „Graz Security Week 2024“, 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 „Toolkit“ konnte auch 2024 einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt.

Der Personalstand ist mit Stand 31.12.2024 im Vergleich zum Vorjahr (31.12.2023) 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 Erträge 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.

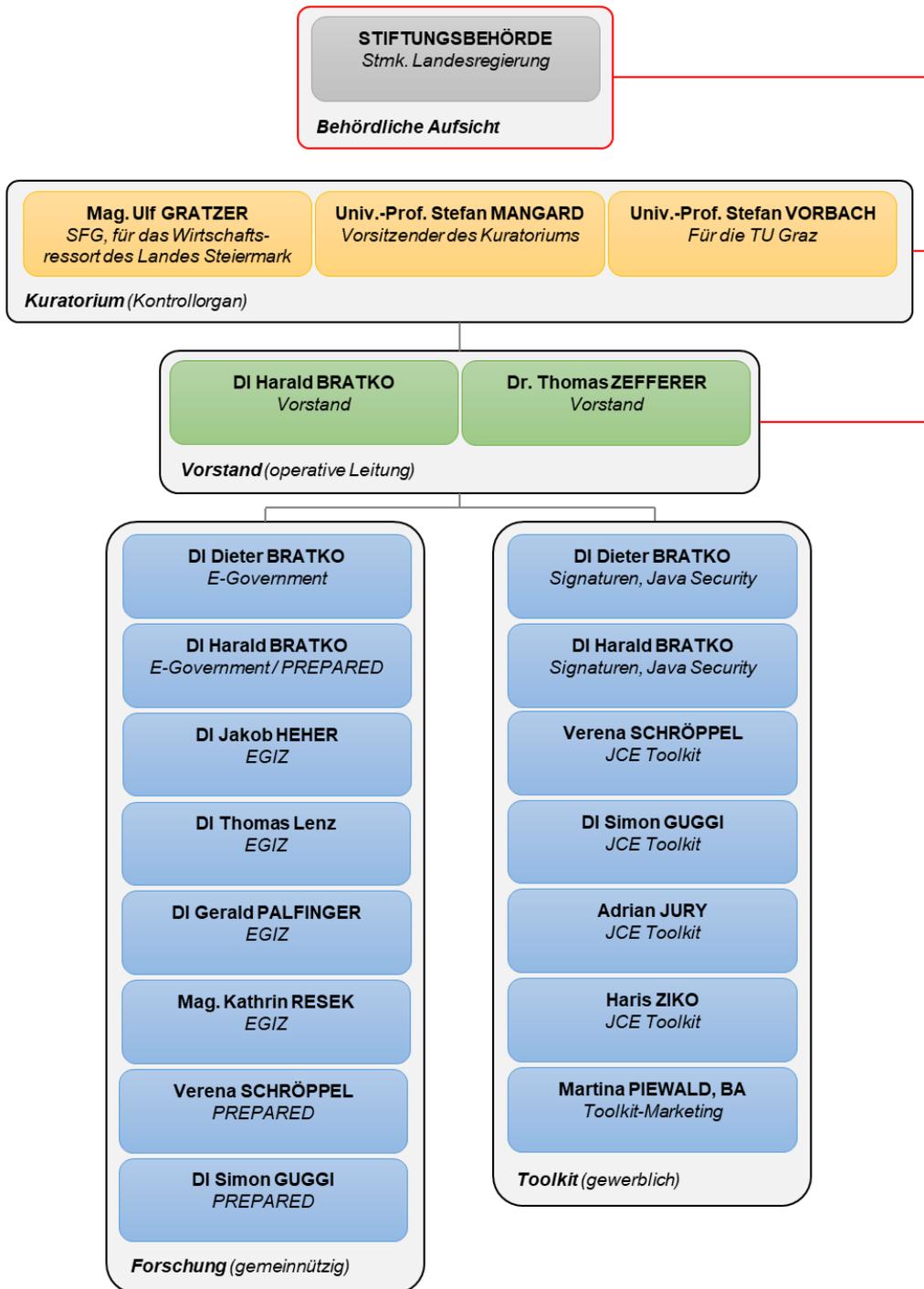
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2024 waren dies:
 - ♦ Mag. Ulf Gratzner (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 31.12.2024 dargestellt. Frau Verena Schröppel, Herr DI Simon Guggi, Herr DI Dieter Bratko und Herr DI Harald Bratko waren 2024 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 31.12.2024

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.

Im Jahr 2024 konnte die Stiftung insbesondere auch Leistungen in den Bereichen Lehre und Wissenstransfer erbringen. Mitarbeiter der Stiftung engagierten sich im Rahmen von Lehrveranstaltungen an der TU Graz im Bereich der angewandten Informationssicherheit.

2.1.1. Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2024 wurden Preise an 15 Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- **Simon Gerhalter** für *“Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks: Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2”* eingereicht und akzeptiert bei der Konferenz ToSC 2024/1 (FSE 2024)
- **Roland Czerny** für *“Generic and Automated Drive-by GPU Cache Attacks from the Browser”* eingereicht und akzeptiert bei der Konferenz AsiaCCS 2024
- **Christoph Gruber** für *„Generic and Automated Drive-by GPU Cache Attacks from the Browser“* eingereicht und akzeptiert bei der Konferenz AsiaCCS 2024
- **Michael Streibl** für *„Whipping the Multivariate-based MAYO Signature Scheme using Hardware Platforms“* eingereicht und akzeptiert bei der Konferenz CCS 2024
- **Florian Krieger** für *„Aloha-HE: A Low-Area Hardware Accelerator for Client-Side Operations in Homomorphic Encryption“* eingereicht und akzeptiert bei der Konferenz DATE 2024
- **Maximilian Mathie** für *„Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems“* eingereicht und akzeptiert bei der Konferenz ARES 2024
- **Christoph Royer** für *„Remote Scheduler Contention Attacks“* eingereicht und akzeptiert bei der Konferenz FC 2024
- **Simone Franza** für *„SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript“* eingereicht und akzeptiert bei der Konferenz USENIX 2024

- **Carina Fiedler** für „*A Systematic Evaluation of Novel and Existing Cache Side Channels*“ eingereicht und akzeptiert bei der Konferenz NDSS 2025
- **Felix Windisch** für „*Synthesis from Infinite-State Generalized Reactivity (1) Specifications*“ eingereicht und akzeptiert bei der Konferenz ISOLA 2024
- **Tobias Hennerbichler** für „*OPRFs from Isogenies: Designs and Analysis*“ eingereicht und akzeptiert bei der Konferenz AsiaCCS 2024
- **Thomas Steinbauer** für „*KernelSnitch: Side Channel-Attacks on Kernel Data Structures*“ eingereicht und akzeptiert bei der Konferenz NDSS 2025
- **Kevin Pretterhofer** für „*Security Aspects of Masking on FPGAs*“ eingereicht und akzeptiert bei der Konferenz HOST 2024
- **Giuseppe La Manna** für „*Secret Spilling Drive: Leaking User Behavior through SSD Contention*“ eingereicht und akzeptiert bei der Konferenz NDSS 2025
- **Hannes Weissteiner** für „*CounterSEveillance: Performance-Counter Attacks on AMD SEV-SNP*“ eingereicht und akzeptiert bei der Konferenz NDSS 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. IAIK Bachelor Excellence Award

Die Stiftung SIC unterstützt den IAIK Bachelor Excellence Award, über den vielversprechende Studierende im Bereich IT-Security nach Nachweis des entsprechenden Studienerfolgs finanziell gefördert werden. Im Jahr 2024 wurde der IAIK Bachelor Excellence Award vier Studierenden zuerkannt. An drei Studierende wurde die mit dem Award verbundene finanzielle Zuwendung (je € 1.000,00) bereits im Jahr 2024 ausbezahlt (€ 3.000,00 gesamt), der vierte Award wird im Jahr 2025 entsprechend ausbezahlt.

2.1.3. TU Graz 100 Stipendien

Im Rahmen des von der TU Graz ins Leben gerufenen Stipendienprogramms „TU Graz 100“ förderte die Stiftung SIC zwei Studierende über Stipendien während ihres Master-Studiums an der TU Graz. Folgende Studierende wurden durch die Stiftung SIC über Stipendien finanziell unterstützt:

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

Nachdem die ersten Tranchen des Stipendiums bereits im Wintersemester 2022/23, im Sommersemester 2023 und im Wintersemester 2023/2024 an die beiden Studierenden überwiesen wurden, erfolgte im Sommersemester 2024 nach Prüfung des Studienerfolgs die Überweisung der verbleibenden Tranche. In Summe wurden im Jahr 2024 damit € 4.000,00 an die beiden Studierenden ausbezahlt.

2.1.4. Graz Security Week 2024

Die Graz Security Week 2024 ist eine wiederholt stattfindende einwöchige Summer School, die sich an Studierende aus dem Bereich IT-Security richtet und der Wissensvermittlung in diesem Bereich

dient. Im Jahr 2024 nahmen über 60 Studierende und über 10 Vortragende an der Summer School teil. Die Stiftung unterstützte die Organisation und Durchführung der Veranstaltung finanziell mit einem Betrag von € 1.048,50.

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 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 ISEC (vormals IAİK) 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 2024 im Schnitt der letzten Jahre. Dies wurde über Aufträge zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdiensteanbieter ergänzt.