stiftung secure information and communication

# Jahresbericht 2007

*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 2007 berichtet.

## 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 15. Mai 2008

# 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 „*... Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen ...*“ erfolgen.

Dieser Jahresbericht 2007 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2007 dar. Der Bericht behält die Struktur der bisherigen Berichte.

Im Berichtszeitraum konnte die Stiftung in allen Bereichen des Stiftungszwecks wertvolle Beiträge leisten:

- Seitens der TU Graz wurde die „*Stiftungsprofessur Informationssicherheit*“, die von der Stiftung SIC initiiert wurde, bereits 2006 in eine permanente Professur übergeführt. Die Stelle von Prof. Vincent Rijmen wird dabei bis 2009 von der Stiftung finanziert, danach bis 2012 in einer Teilfinanzierung.

- Aus dem Bereich Lehre wurde eine Lehrveranstaltung „*Kritische Informationsinfrastrukturen*“ an der TU Graz finanziert. Diese Lehrveranstaltung wird im Wintersemester 2007/2008 zum zweiten Mal abgehalten.

- Die 2005 mit der Firma NXP (vormals Philips) gestartete Initiative „*Programme for Advanced Contactless Technology*“ (PROACT) wurde bis Juli 2007 fortgeführt. Es wurde eine Spring School organisiert bzw. wurden aus der Initiative einige Diplomarbeiten aus dem Bereich Radio Frequency Identification (RFID) gestartet.

- Im Bereich E-Government hat sich die Stiftung zusammen mit der TU Graz an Projekten des Landes Steiermark und des Bundes beteiligt.

- Das von der EU geförderte Forschungsprojekt POSITIF zu Intrusion Detection, an dem die Stiftung beteiligt war, wurde erfolgreich abgeschlossen.

- Aus dem Hilfsbetrieb JCE Toolkit konnten wiederum Gewinne erzielt werden, 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 2007 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 25. April 2008 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 wie folgt definiert:

> *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 durch Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen, die zur Erreichung des Stiftungszweckes beitragen. Diese stellen den begünstigten Personenkreis gemäß § 10 Abs. 2 Z 3 des Steiermärkischen Stiftungs- und Fondsgesetzes dar.*
>
> *Die Leistungen der Stiftung erfolgen aus den Erträgnissen des Stiftungsvermögens bzw. aus dem Stiftungsvermögen selbst. Sämtliche Leistungen der Stiftung sind freiwillig und begründen keinen Rechtsanspruch gegen die Stiftung. Über die Gewährung von Leistungen der Stiftung entscheiden die Organe der Stiftung.*

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 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
- 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

In den bisherigen fünf Jahren ihres Bestehens ist es der Stiftung gelungen, über Forschungsförderungen, Zuwendungen, Kooperationen und Gewinne des Hilfsbetriebs Toolkit Leistungen in einem Ausmaß zu erbringen, die deutlich über den reinen Ertrag des Stammvermögens hinausgehen. Es konnten Rücklagen gebildet werden, die auch in absehbarer Zukunft einen kontinuierlichen Betrieb der Leistungen am derzeit quantitativ und qualitativ hohen Niveau oder auch Investitionen in neue Forschungsgebiete erlauben, ohne noch auf das Stammvermögen zurückgreifen zu müssen.

Im Berichtszeitraum 2007 wurde im Bereich der gemeinnützigen Leistungen wieder eine Reihe von Aktivitäten finanziert. Leistungen aus dem Stiftungszweck mit Impulsen in der Ausbildung der Studierenden an der TU Graz waren vor allem die weitere Finanzierung der Stiftungsprofessur Kryptographie und die Vorlesung zu kritischen Informationsinfrastrukturen. Damit wurde der Ausbau der Kryptographie in Graz unterstützt bzw. ein neuer Bereich erschlossen. In der eigenständigen Forschung wurde das EU Forschungsprojekt POSITIF mit dem finalen Review erfolgreich abgeschlossen.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Angesichts des geringen Personalstands in der Stiftung selbst wurden wissenschaftliche Weiterentwicklungen und notwendige Support- und Wartungsaufgaben an die TU Graz vergeben.

## 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 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.

## 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 2007 waren dies:

- Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
- o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
- o.Univ.-Prof. Dr. Hans Sünkel (für die TU Graz)

▪ Staatliche Aufsicht ist die Stiftungsbehörde der Steiermärkischen Landesregierung

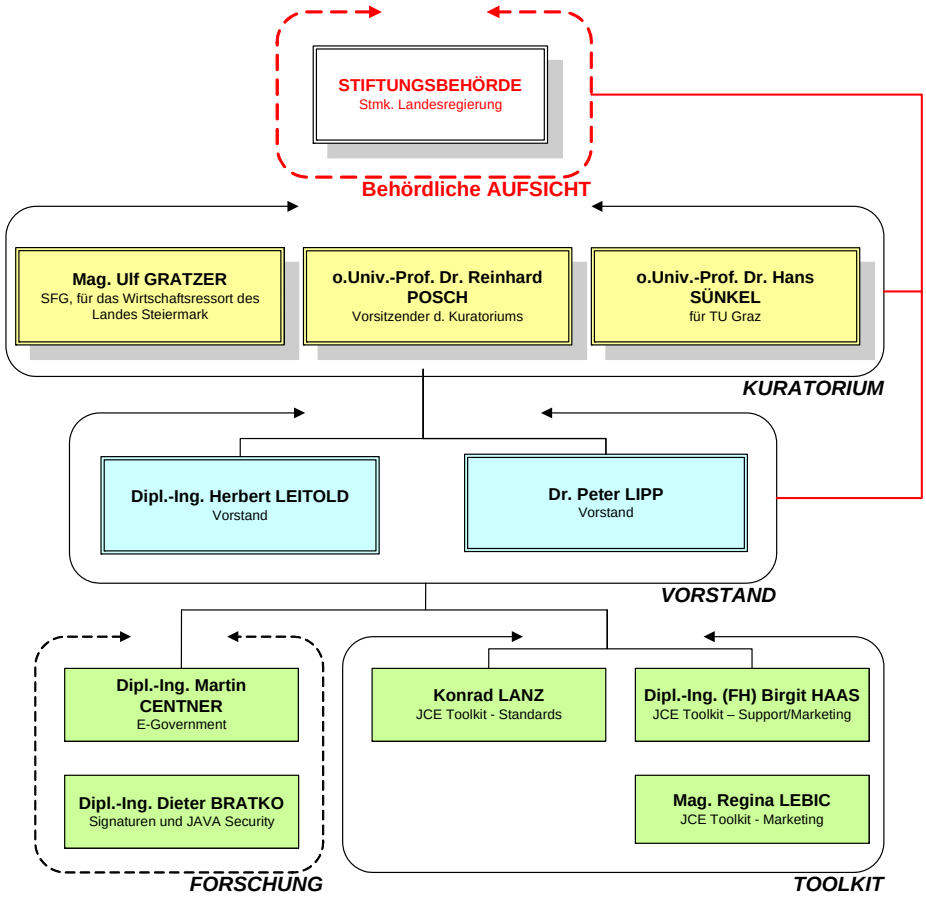
o Die Führungsebene bildet der Vorstand

- Dipl.-Ing. Herbert Leitold
- Dr. Peter Lipp

o 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 31.12.2007 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.




Organigramm und Personalstand per 31.12.2007

# 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*“ und „*Eigenständige Forschung und Entwicklung*“ strukturiert berichtet.

## *2.1 Förderung von Forschung und Lehre, Wissenstransfer*

### 2.1.1 Stiftungsprofessur Informationssicherheit

Seit 1.10.2004 ist die Stiftungsprofessur Informationssicherheit mit Prof. Dr. Vincent Rijmen besetzt. Dabei finanziert die Stiftung die Personalkosten von Prof. Rijmen, die TU Graz stattet die Stiftungsprofessur mit Räumlichkeiten, Assistenten und Sekretariat aus.

Seit 2006 ist die Professur an der TU Graz permanent eingerichtet. Die Stiftung hat eine Finanzierungszusage bis 2009 bzw. eine Teil-Finanzierungszusage bis 2012 gegeben.

Seit Oktober 2007 ist die Stiftungsprofessur an der TU Graz nur mehr zu 40 % besetzt, die Initiative besteht jedoch weiter und 2007 konnte die Gruppe zahlreiche wissenschaftliche Schriften veröffentlichen oder war Co-Autor von wissenschaftlichen Publikationen:

1. Babbage, S.; Cid, C.; Pramstaller, N.; Raddum, H.: *An Analysis of the Hermes8 Stream Ciphers.* in: Proceedings of the 12th Australasian Conference on Information Security and Privacy - ACISP 2007 (2007), S. 1 - 10. Australiasian Conference on Information Security and Privacy.

2. Daemen, J.; Rijmen, V.: *Plateau characteristics*. in: IET information security (2007), S. 11 - 18

3. Daemen, J.; Rijmen, V.: *Probability distributions of correlations and differentials in block ciphers.* in: Journal of mathematical cryptology 1 (2007) 3 , S. 221 - 242

4. De Cannière, C.; Mendel, F.; Rechberger, C.: *Collisions for 70-step SHA-1: On the Full Cost of Collision Search.* in: Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers. (2007), S. 56 - 73

5. Knudsen, L. R.; Rechberger, C.; Thomsen, S. S.: *The Grindahl hash functions.* in: Fast Software Encryption (FSE) (2007), S. 39 - 57. Fast Software Encryption Workshop

6. Knudsen, L. R.; Rijmen, V.: *Known-key distinguishers for some block ciphers.* in: International Conference on the Theory and Application of Cryptology and Information Security; (2007), S. 315 – 324

7. Mendel, F.; Lano, J.; Preneel, B.: *Cryptanalysis of Reduced Variants of the FORK-256 Hash Function.* in: Topics in Cryptology – CT-RSA 2007 (2007), S. 85 - 100. Cryptographers´ Track at the RSA Conference; 2007

8. Mendel, F.; Rechberger, C.; Rijmen, V.: *Secure enough? Re-assessment of the world's most-used hash function.* in: iSGTW - International science grid this week, 2007

9. Mendel, F.; Rijmen, V.: *Colliding Message Pair for 53-Step HAS-160.* in: International Conference on Information Security and Cryptology; (2007), S. 324 - 334

10. Mendel, F.; Rijmen, V.: *Cryptanalysis of the Tiger Hash Function.* in: International Conference on the Theory and Application of Cryptology and Information Security; (2007), S. 536 - 550

11. Mendel, F.; Rijmen, V.: *Weaknesses in the HAS-V Compression Function.* in: International Conference on Information Security and Cryptology; (2007), S. 335 – 345

12. Pramstaller, N.; Lamberger, M.; Rijmen, V.: *Second Preimages for Iterated Hash Functions and their Implications on MACs.* in: Proceedings of the 12th Australasian Conference on Information Security and Privacy - ACISP (2007), S. 68 - 81. Australiasian Conference on Information Security and Privacy

13. Rechberger, C.; Rijmen, V.: *On Authentication With HMAC and Non-Random Properties*. in: Financial Cryptography (2007), S. 119 - 113. International Conference on Financial Cryptography and Data Security;

14. Rechberger, C.; Rijmen, V.: *The SHA Family of Hash Functions: Recent Results*. in: Proceedings of Security and Protection of Information (2007), S. 107 - 114. Security and Protection of Information Conference; 2007

15. Rijmen, V.; Pramstaller, N.: *Cryptographic Algorithms in Constrained Environments*. in: Wireless Security and Cryptography: Specifications and Implementations. (2007), S. 177 – 211

Die Forschung zu Kollisionen von SHA-1 wurde 2007 fortgesetzt. SHA-1 ist eine der wesentlichsten Hash-Funktionen im Bereich der elektronischen Signatur. An einer von der Gruppe um Prof. Rijmen gestarteten, übers Internet verteilten Suche nach Kollisionen waren Ende 2007 bereits etwa 5.000 Benutzer und etwa 10.000 Rechner beteiligt.

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „Angewandte Kryptographie“ und „Angewandte Kryptographie 2“, „Einführung in die Informations-sicherheit“ und „IT-Sicherheit“ betreut. Das Angebot wird mit Seminaren, Projekten und Diplomarbeiten ergänzt.

Weiters konnte 2007 Dr. Norbert Pramstaller seine Dissertation „Cryptanalysis and Design of Iterated Hash Functions“ erfolgreich abschließen.

Die von der Stiftung finanzierte Professur ist also als Nukleus erstklassischer Forschung im Bereich der Kryptographie anzusehen. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die mittlerweile internationales Ansehen genießt.

### 2.1.2 Vorlesung Kritische Informationsinfrastrukturen

Bereits im Wintersemester 2006/2007 wurde eine Vorlesung zu kritischen Informationsinfrastrukturen an der TU Graz gestartet und von der Stiftung finanziert. Mit Dr. Otto Hellwig konnte ein Vortragender gewonnen werden, der aus seiner beruflichen Tätigkeit als Chief Information Officer im Bundeskanzleramt eine reichhaltige Erfahrung

in diesem, angesichts der zunehmenden Abhängigkeit von Informationstechnologien immens in der Bedeutung steigenden Bereich, mitbringt.

Es wurde damit den Studierenden der TU Graz eine Bereicherung der Möglichkeiten in einem Feld angeboten, das erst an sehr wenigen Universitäten unterrichtet wird. Damit leistet die Stiftung einen Beitrag, Studierende konkurrenzfähig auszubilden.

Die Vorlesung Kritische Informationsinfrastrukturen wird von der TU Graz auch im Wintersemsemester 2007/2008 angeboten. Unter anderem hat die Stiftung in diesem Lehrgang den Studierenden eine Exkursion in das Zentrale Ausweichsystem des Bundes in St. Johann ermöglicht.

### 2.1.3 RFID-Initiative PROACT

Die Initiative „*Programme for Advanced Contactless Technology*“ (PROACT) wurde über eine Förderung von NXP (vormals Philips) im Jahr 2005 an der TU Graz eingerichtet. Dabei hat die Stiftung die Mittel verwaltet, die nach Arbeitsprogrammen eines Koordinierungskomitees vergeben wurden.

Eine erfolgreiche Aktivität war eine Spring-School, die vom 18.-20. April 2007 mit 71 TeilnehmerInnen in Graz organisiert wurde. Es wurden den Studierenden an den drei Tagen von vierzehn auch internationalen Vortragenden ebenso viele Sessions zu jeweils 45 oder 90 Minuten geboten, die ein breites Feld der aktuellen Entwicklungen im Bereich RFID abdeckten.

Neben der Förderung von Forschungsprojekten an Instituten der TU Graz konnten aus PROACT auch einige Studentenarbeiten (Bakkalaureats-, Diplom-, und Masterarbeiten) an der TU Graz gestartet werden. Dies waren vier im Jahr 2007 gestartete bzw. zusätzlich zehn im Jahr abgeschlossene Arbeiten (für eine aktuelle Liste konkreter Arbeiten siehe http://proact.tugraz.at/education/theses/index.htm).

Im Juli 2007 wurden Leitung und noch verbliebene Mittel der Initiative PROACT an das Institut für Grundlagen und Theorie der Elektrotechnik (IGTE) der TU Graz übertragen. Damit ist das Projekt in der Stiftung abgeschlossen. PROACT kann als ein wesentlicher Impuls in Lehre und Forschung zu RFID in der Steiermark angesehen werden.

### 2.1.4 E-Government

Mitarbeiter 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.

Die Stiftung hat zusammen mit der TU Graz 2005 den Zuschlag einer Ausschreibung des Landes Steiermark zu Wissenstransfer und Koordination zu E-Government erhalten[1]. Diese Aktivität ist 2006 gestartet und wurde 2007 weitergeführt. Es werden hier bis 2010 zusammen mit der TU Graz je nach Abruf ¼ - ½ Person für E-Government Aktivitäten des Landes Steiermark gestellt. Die Aktivität wird vornehmlich von der TU Graz getragen, es wurden nach notwendiger Expertise Mitarbeiter der Stiftung beigezogen.

[1] Teil 1 der Ausschreibung „GZ FA1B B1.40-5688/2005 Ressourcen für die Konzeption und Umsetzung von E-Government“

## 2.2 Eigenständige Forschung und Entwicklung

### 2.2.1 Forschungsprojekt POSITIF

Die Stiftung hat im 6. EU Rahmenprogramm im Forschungsprojekt „*Policy-based Security Tool and Framework (POSITIF)*“ teilgenommen. Das Projekt hatte eine Laufzeit von dreieinhalb Jahren und wurde im Juli 2007 mit dem finalen Review abgeschlossen. Die inhaltlichen Teile der Stiftung wurden bereits 2006 fertig gestellt, weshalb sich dieser Abschnitt auf den Bericht des erfolgreichen formellen Abschlusses des Gesamtprojekts beschränkt.

### 2.2.2 Forschung zu elektronischen Signaturen

Mitarbeiter der Stiftung haben 2007 im Bereich der Anwendungen elektronischer Signaturen geforscht. Dabei wurden folgende Aktivitäten durchgeführt:

- Integriertest Testen von Signaturanwendungskomponenten
  Hier lag der Schwerpunkt auf der Erforschung von Mechanismen zur Automatisierung der Durchführung zahlreicher positiver und negativer Testfälle, insbesondere auch mit Eignung zum Testen fortgeschrittener elektronischer Signaturen.

- Kompatibilität der Implementierungen elektronischer Signatur-Standards
  Hierbei wurde die Interoperabilität mit anderen Implementierungen von Signaturstandards verglichen und die mit der Implementierung von Signaturstandards verbundenen Probleme erforscht.

- CAdES: Die Softwarebibliothek der Stiftung SIC hat bisher ausschließlich den XAdES-Standard (XML) für elektronische Signaturen umfasst. Ein weiterer Standard (ASN.1, CAdES) wurde auf Eignung hin untersucht.

## 2.3 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.

### 2.3.1 Technische Infrastruktur

Die technischen Anlagen der Stiftung, wurden 2007 nur um einen Laptop ausgeweitet. 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.

### 2.3.2 Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb haben sich 2007 etwas unter den Erwartungen entwickelt. Es wurden wiederum Entwicklungen teilweise von eigenem Personal der Stiftung, teilweise durch Forscher des IAIK übernommen. Dabei wurde das Toolkit vor allem wissenschaftlich weiter entwickelt, um über neue Funktionalitäten den Kundenerwartungen nach Unterstützung aktueller Entwicklungen der Informationstechnologie zu genügen.

Ein wesentlicher Erfolg war die nunmehr schon zweite Zertifizierung des Produkts nach dem Standard Common Criteria. Von einer japanischen Zertifizierungsstelle wurde im Juli 2007 dem Produkt ein international anerkanntes Zertifikat nach Evaluierungsstufe „EAL3“ verliehen (siehe Anhang D: Common Criteria Zertifikat). Dieses Zertifikat bestätigt die hohe technische Qualität des Toolkits.

## Anhang: Common Criteria Zertifikat

Dem von der Stiftung betriebenen JCE Toolkit wurde 2007 ein Common Criteria Zertifikat nach der Evaluierungsstufe EAL 3 verliehen.

Japan IT Security Evaluation and Certification Scheme

# Certificate

is awarded to

Certification Number: C0107

**Stiftung Secure Information and Communication Technologies SIC**

**Product Name: IAIK-JCE CC Core**

**Version: 3.15**

**Type of IT Product: IT Product (cryptographic library)**

Evaluation Criteria:
- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)

Evaluation Methodology:
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Assurance Level: EAL3

Protection Profile Conformance: None

Name of CCTL: TÜV Informationstechnik GmbH Evaluation Body for IT-Security

Date of Certification: June 27, 2007

The IT product identified in this certificate has been evaluated at an approved evaluation facility established under the Japan IT Security Evaluation and Certification Scheme using the *Common Methodology for Information Technology Security Evaluation Version2.3(ISO/IEC 18045:2005)*, for conformance to the *Common Criteria for Information Technology Security Evaluation Version2.3(ISO/IEC 15408:2005)* . This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification/validation report. This evaluation has been conducted in accordance with the provisions of the Japan IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.
The misuse of this certificate, including its use regarding the IT Product or system or PP of a version differing from that appearing in this certificate or the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Original Signed

Buheita Fujiwara
Chairman

Date : July 20, 2007

Information-technology Promotion Agency, Japan